VIVOTEK

A Delta Group Company

Version 1

FACE RECOGNITION ACCESS CONTROL SYSTEM

VIVOTEK

Face Manager Server

Instructions for use

September 2020

VIVOTEK

Face Manager Server – User Manual

VIVOTEK INC.
6F, No.192, Lien-Cheng Rd., Chung-Ho, New Taipei City, 235, Taiwan, R.O.C.
|T: +886-2-82455282|F: +886-2-82455532|E: sales@vivotek.com

VIVOTEK USA, INC.
2050 Ringwood Avenue, San Jose, CA 95131
|T: 408-773-8686|F: 408-773-8298|E: salesusa@vivotek.com

VIVOTEK Europe
Zandsteen 15, 2132 MZ Hoofddorp Delta Electronics
T: +31 (0)20 800 3817 E: saleseurope@vivotek.com

Table of Contents

Chapter 1

1. VIVOTEK Face Manager Introduction

Simplify face recognition device management, unify face database and face recognition report

VIVOTEK Face Manager is a security-enhanced face recognition system data integrator designed to facilitate the management of face recognition devices, authority control and compilation of face recognition data for complete attendance and access control reports.

VIVOTEK Face Manager acts as a unified portal, allowing users of face recognition devices/servers and managing the face data of registered persons, assigning access rights to each registered person and viewing face recognition reports under a single interface.

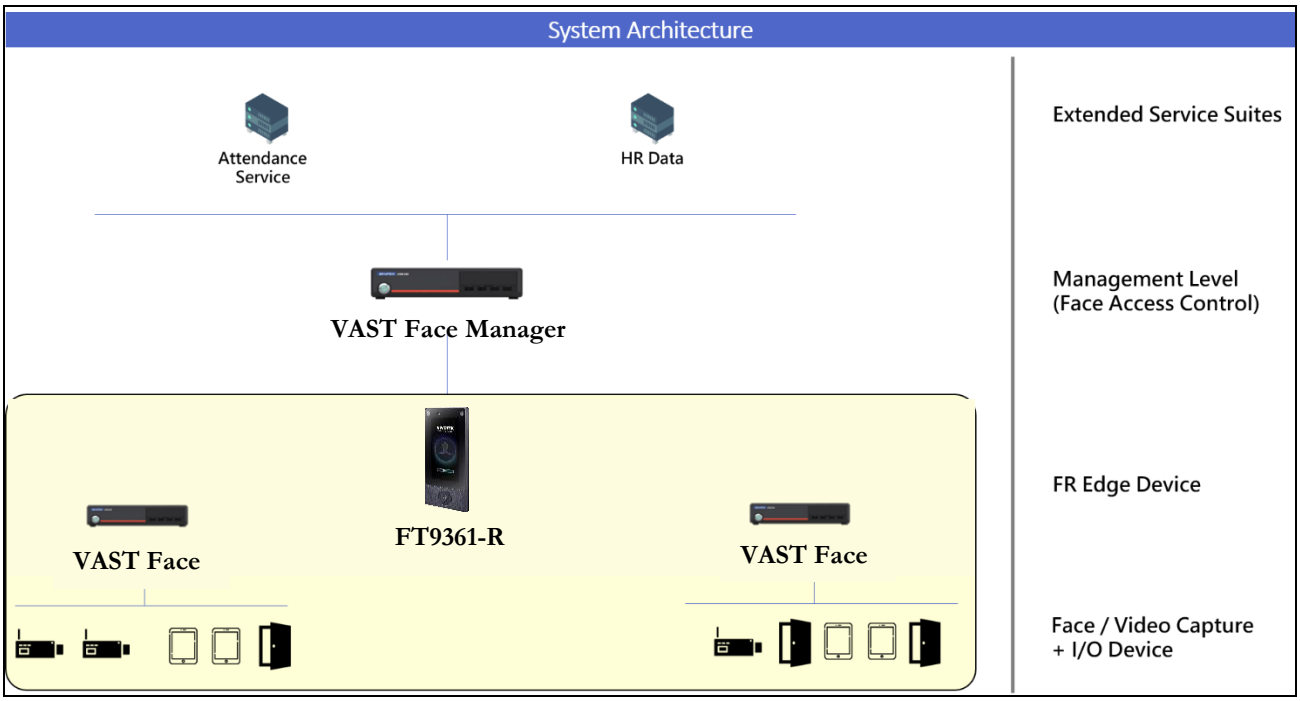


FIGURE 1.1 Overall Face Manager System design.

1.1 How VAST Face Manager works

VIVOTEK Face Manager integrates multiple brands (owned and third-party) of face recognition devices on a single platform, enabling system users to centralize face data, access control policies, face recognition reports, simplify device management, and trigger operations based on face recognition settings. Supported devices include face recognition servers and face recognition tablets; all face recognition tablets are integrated through the use of SDKs from face recognition tablet manufacturers.

When a face recognition device is connected to Face Manager, its local face database will be automatically synced to Face Manager's database. Similarly, all face recognition events (stranger, VIP, blacklist) will be forwarded to Face Manager to generate reports or trigger user-defined actions based on specific face/group data.

If integration with other systems is required, Face Manager comes with a RESTful JSON API that allows third-party developers to construct and receive face recognition events or manage face data through Face Manager.

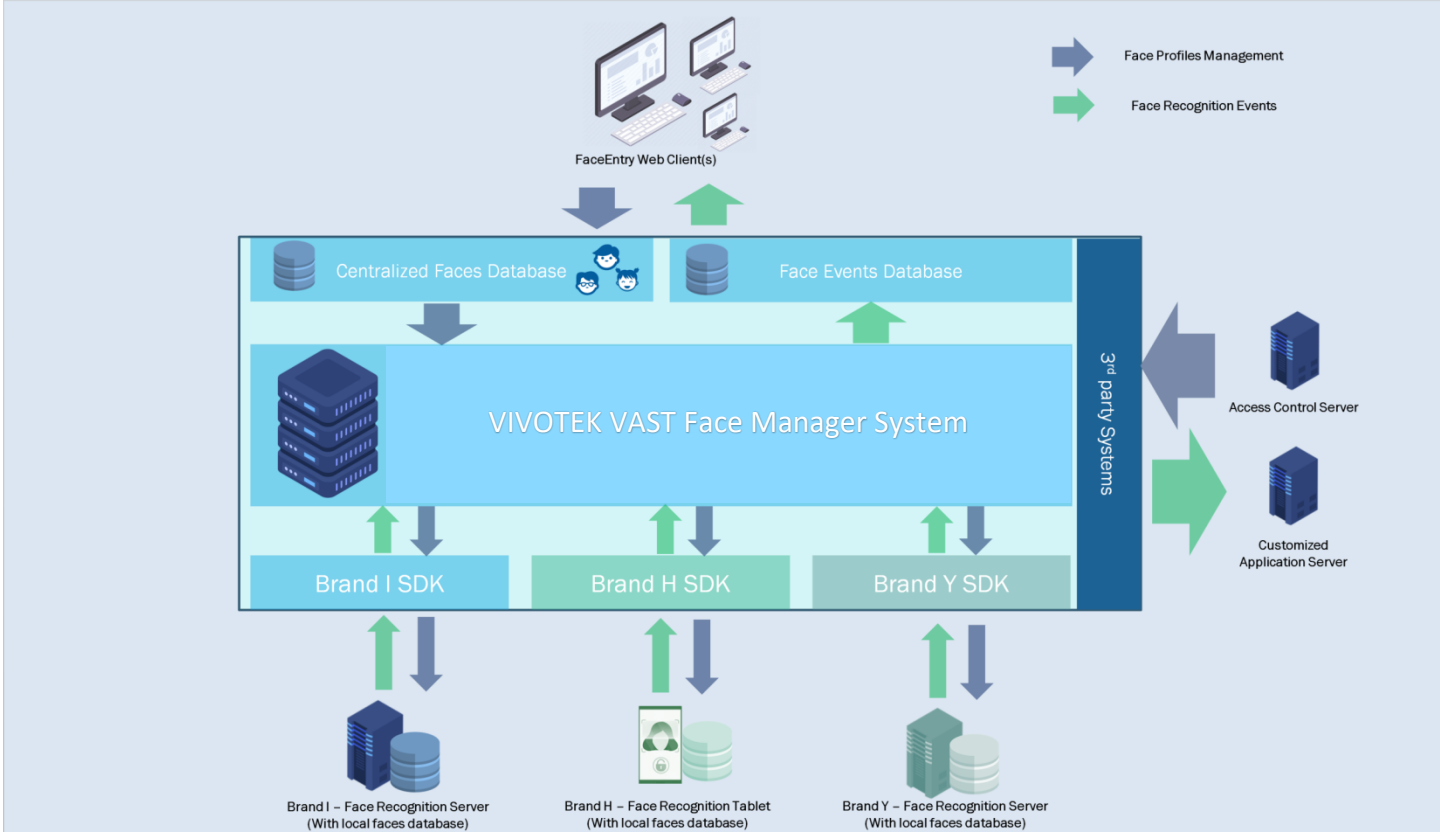


FIGURE 1.2 Face Manager System Design.

1.2 System Architecture

VIVOTEK Face Manager is a system based on docker Container running on Linux Ubuntu. The Face Manager system is not a single service application but an integration of distributed components.

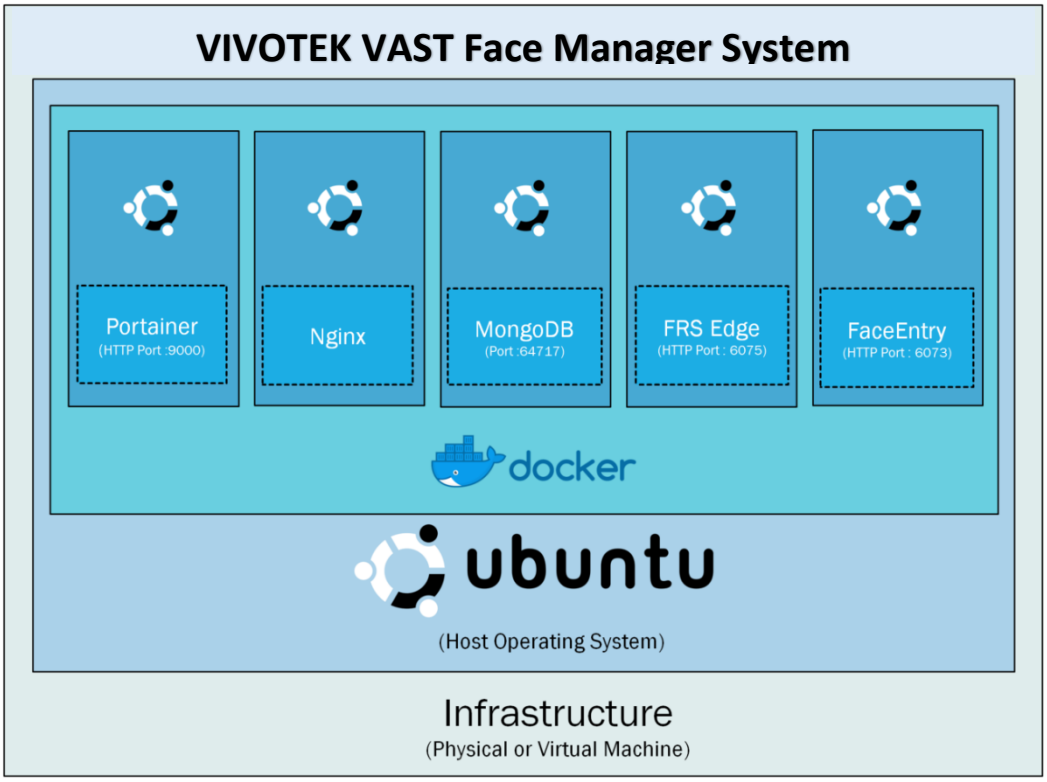


FIGURE 1.3 Face Manager System Architecture.

System Components	Use
Linux Ubuntu OS	Operating system for hosting docker and container
Docker	OS-level virtualization platform designed to run Container-based applications
Portainer Docker	UI management interface for docker Container
MongoDB	NO-SQL database engine for storing face profile data, face recognition events, logs and system configuration of registered personnel
Nginx	Web reverse proxy for redirecting traffic from any underlying Container to a specific interface/protocol
VAST FACE Edge	Local face recognition server for verifying whether a person is blacklisted or registered
Face Manager	The primary application server is responsible for. • Centrally Hosted Face Database • Synchronize face data with underlying connected face recognition devices • Acts as a gateway to receive face recognition events from all devices • Triggers user-defined actions based on face recognition events • Provides integration with external systems

1.3 Face Manager System Requirements

In order to ensure stable system operation, the following are the minimum specifications for the hardware and software required for the Face Manager system

System Components	Minimum requirement specification
Quantity	• One Mainframe
Operating System	• Ubuntu 16.04 Server
CPU	• Intel Core i5 8th generation or newer, Xeon Silver,or equivalent (Min 4 vCPU if using virtual machines)
Memory	• At least 16 GB RAM
Operating System Hard Drive	• At least 250 GB
Data Hard Drive	• At least 500 GB
Network Card	• Ethernet RJ45 100 Mbps
Resolution	• 1920 * 1080 pixels

Remark

- VIVOTEK Face Manager can be installed directly on a PC or a virtual machine, the latter being more convenient to manage and therefore the recommended choice.

1.4 Face Manager Features

Face Manager allows users to centrally manage any brand of face recognition system/device under one umbrella platform, therefore, the platform provides users with the flexibility to choose their preferred type of face recognition devices.

Similarly, Face Manager acts as a face database hub to which all controlled face recognition devices can synchronize their databases. The user does not need to consider the brand or physical location of the underlying face recognition system to plan Face Manager so that it can trigger system operations based on specific face data or groups.

Even though Face Manager stores an organization's entire face profile database, the system administrator can segregate the data according to system roles, each with different functions; thus any given user can only view or edit the face data that he or she is authorized to manage.

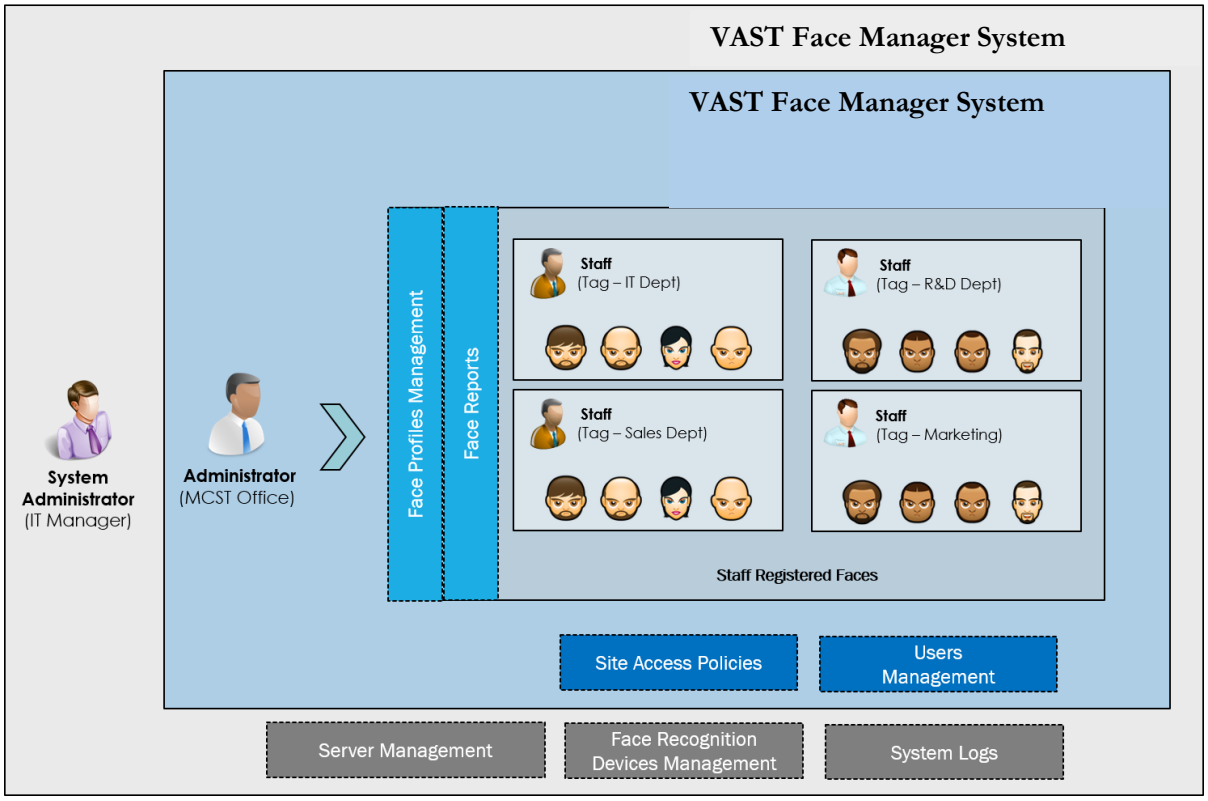


FIGURE 1.4 Face Manager system users' roles with data segregation

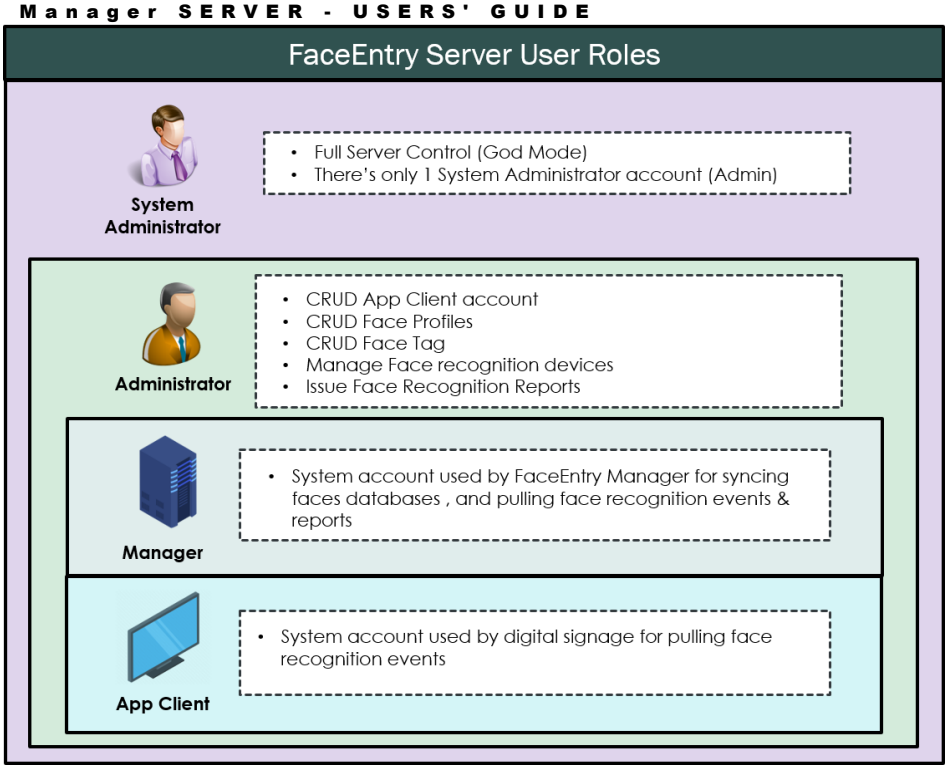


FIGURE 1.5 Face Manager system users' roles and functions

Similar to traditional card access systems, Face Manager allows Administrators to define face recognition devices in which registered personnel can be authenticated based on a specific face profile or group. Similarly, after creating a person's face profile, Face Manager will assign a unique virtual card number to identify that person.

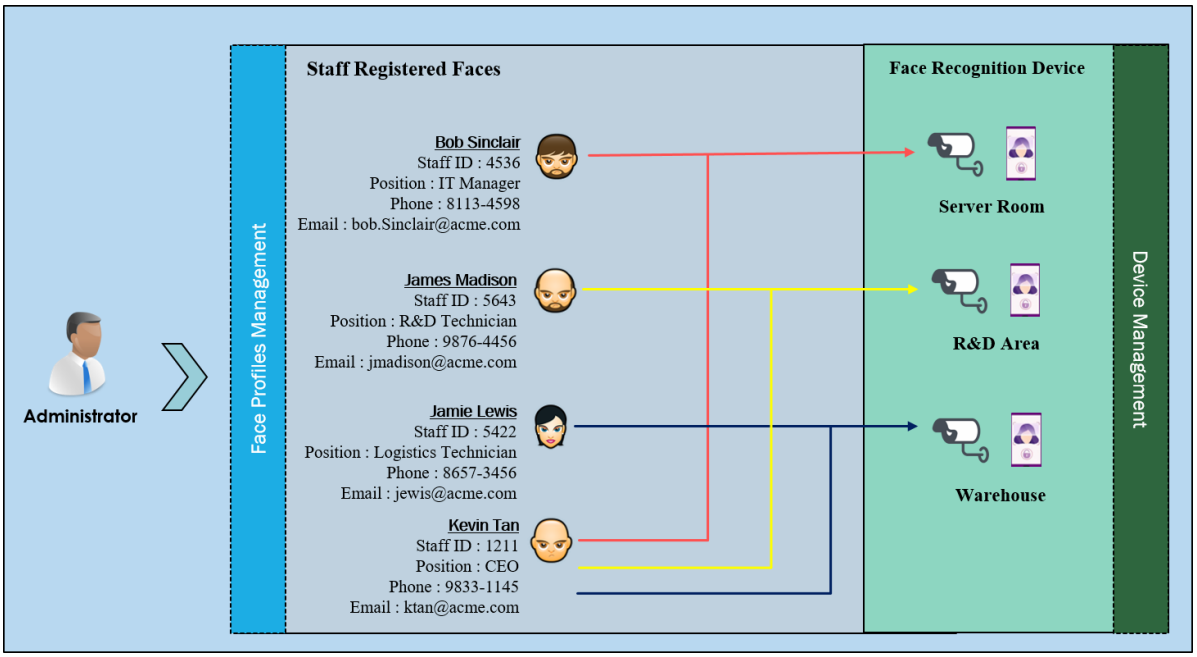


FIGURE 1.6 Face Manager Enrolled profiles access permission

Chapter 2

2. Face Manager Server Operation

This chapter describes how to use the Face Manager server for basic operations

2.1 Basic server operation

2.1.1 Create Face Manager users

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page
2. Enter your System Admin login credentials and click Login.
3. Navigate to the "Account" menu and click "+Create"
4. The "Create Account" menu will be displayed, and provide the following information:
    a. Username ➡ Enter the new Face Manager user account
    b. Password ➡ Enter the new Face Manager user password
    c. Confirm Password ➡ Confirm the new Face Manager account password
    d. Name ➡ Enter the name of the owner of the new Face Manager account
    e. Role ➡ Select "Administrator"
    f. Email ➡ Enter the email of a new Face Manager user
    g. All other fields are optional.

Remark

- System Admin can create Administrator, Manager and App Client role accounts.
- Administrator role accounts can only create App Client role accounts.

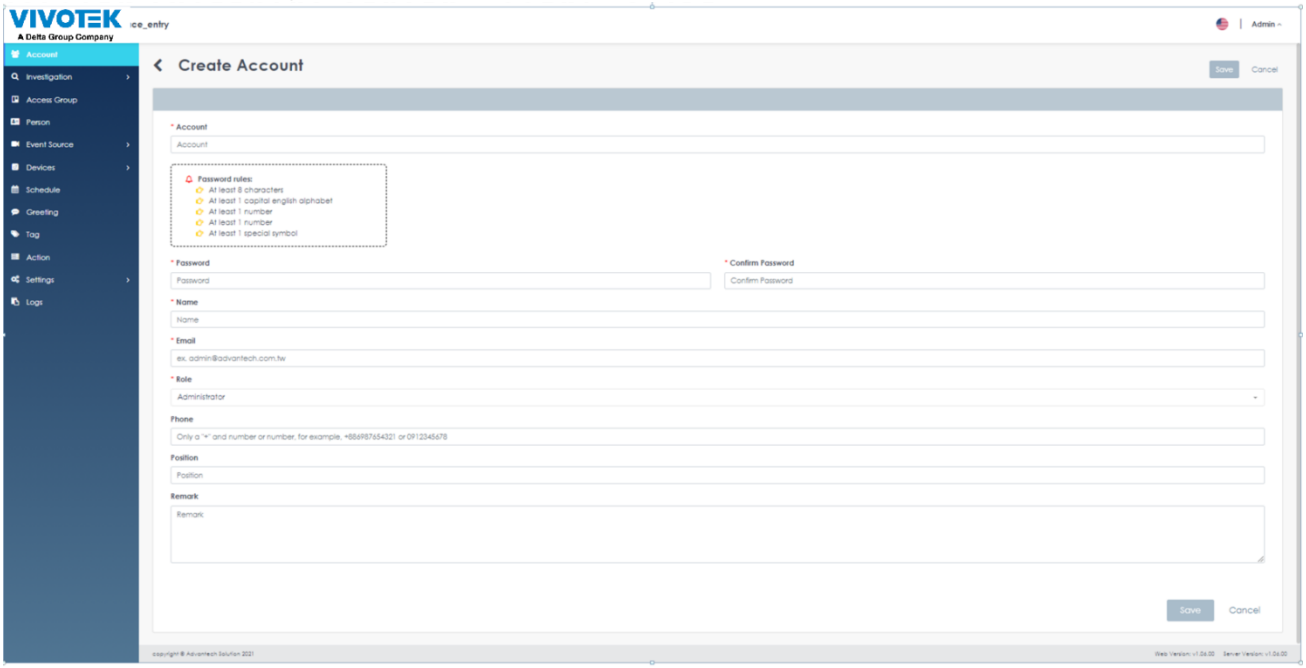


FIGURE 2.1 Face Manager server New Administrator Account

5. Click "Save" to create an account
6. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page
7. Enter your Administrator login credentials and click Login.
8. Navigate to the "Account" menu and click "+Create"
9. The "Create Account" menu will be displayed, and providee the following information:
    a. Username ➡ Enter a new Face Manager user account
    b. Password ➡ Enter the new Face Manager user password
    c. Confirm Password ➡ Confirm the new Face Manager account password
    d. Name ➡ Enter the name of the owner of the new Face Manager account
    e. Role ➡ Select"App Client" (App Client settings will appear after selection)
    f. Email ➡ Enter the email of a new Face Manager user
    g. All other fields are optional.

10. App Client Setting Items:
    a. Image source➡Select face recognition image source
    b. Greeting➡Select from configured greetings (Click the + sign in the upper right corner after selection to set more than one)
    c. Title➡Set the greeting title
    d. Theme Style ➡Choose from "Light Style" or "Dark Style"
    e. Font Size ➡Choose from "Large", "Medium" or "Small"
    f. Font Color ➡ You can enter your own color code
    g. Recognition result display time ➡ The display time of the welcome message after a successful recognition
    h. Background images ➡can be uploaded and can preview the effect of the settings
11. Click "Save" to create an account

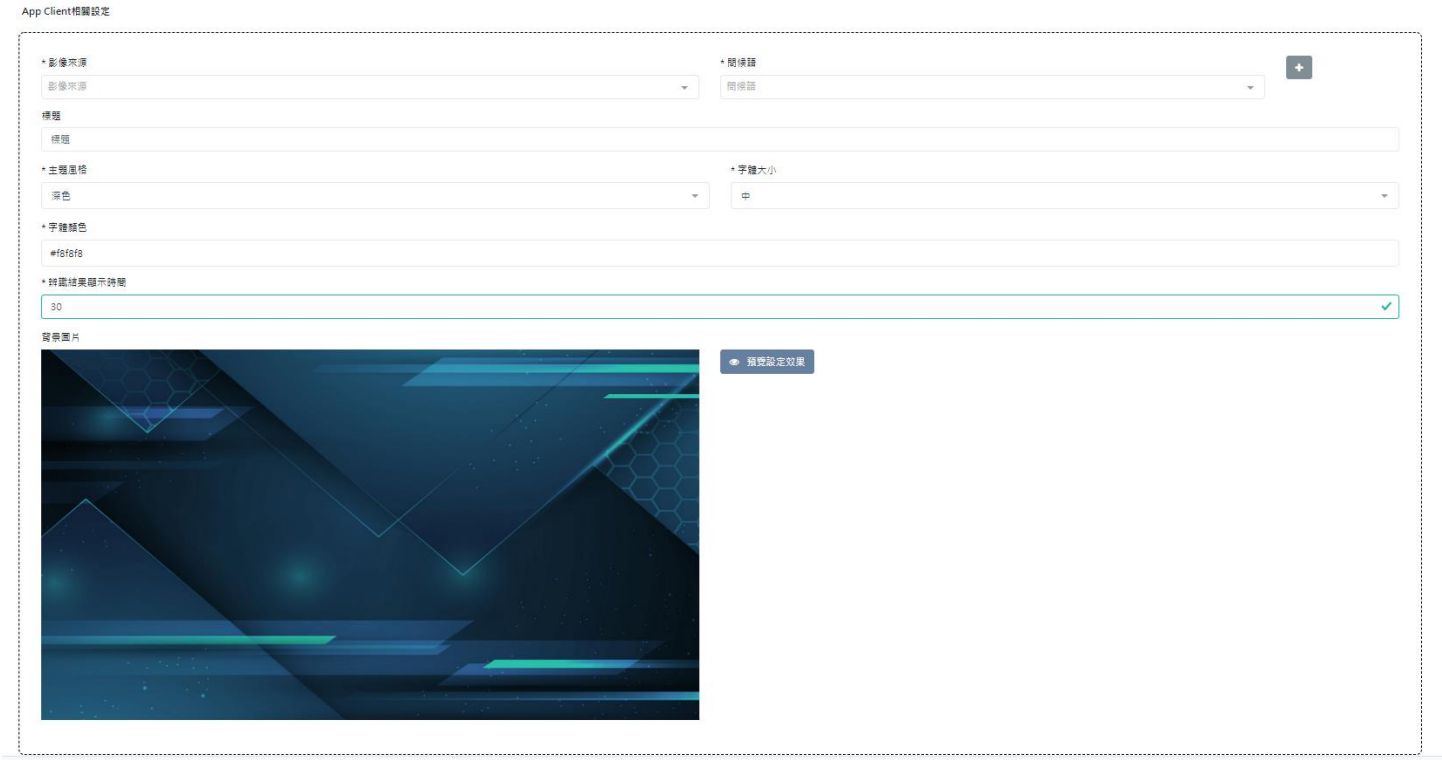


FIGURE 2.2 Face Manager server App Client Account

2.1.2 Modify user account password

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Enter your login credentials and click "Login".
3. Click on the avatar icon in the upper right corner to display the user's personal information
4. Click on the "Change Password" icon , which is represented by a key

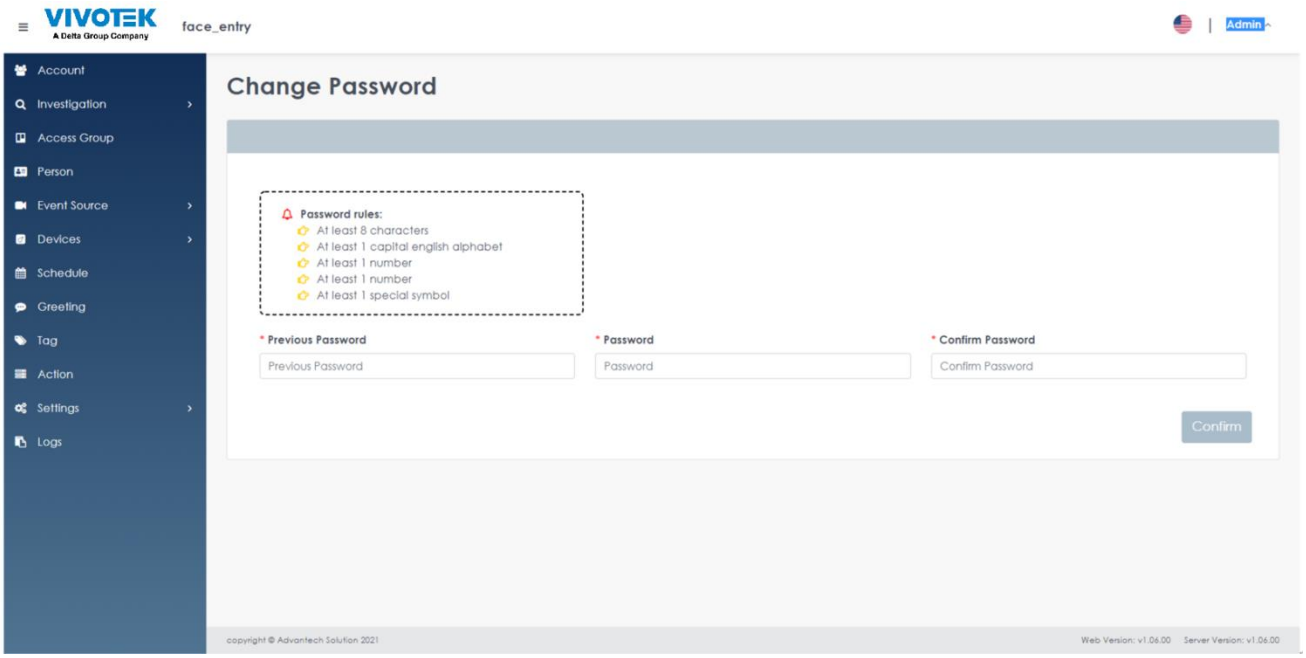


FIGURE 2.3 Face Manager server User profile settings

5. Enter the user's current password, a new password, and confirm the new password
6. Click "Save" to apply changes
7. Login to Face Manager server with new password

2.1.3 Resetting the password

Remark

- In order to reset the user password, SMTP email must be set up and connected to the Face Manager server beforehand (see Section 2.11.4)

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Click on the "Forgot Password" link
3. On the "Verify Account" page, enter the user account and its associated email address to reset the password
4. Click on "Get Verification Code"

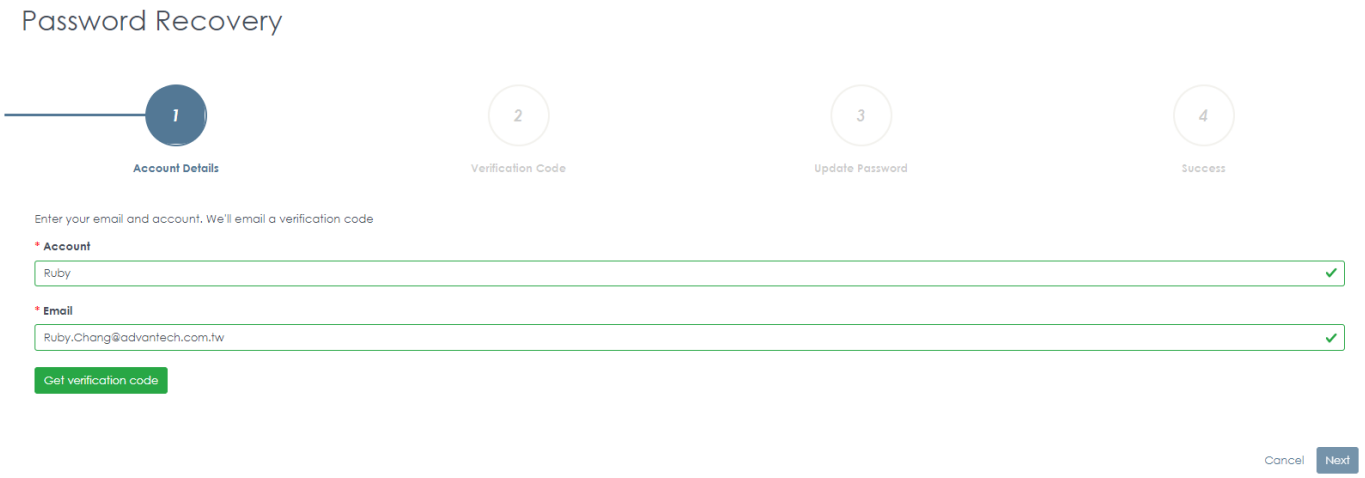


FIGURE 2.4 server Get recovery code page

5. Click "Next"
6. Check the email associated with the user account and wait a few minutes for the password reset email

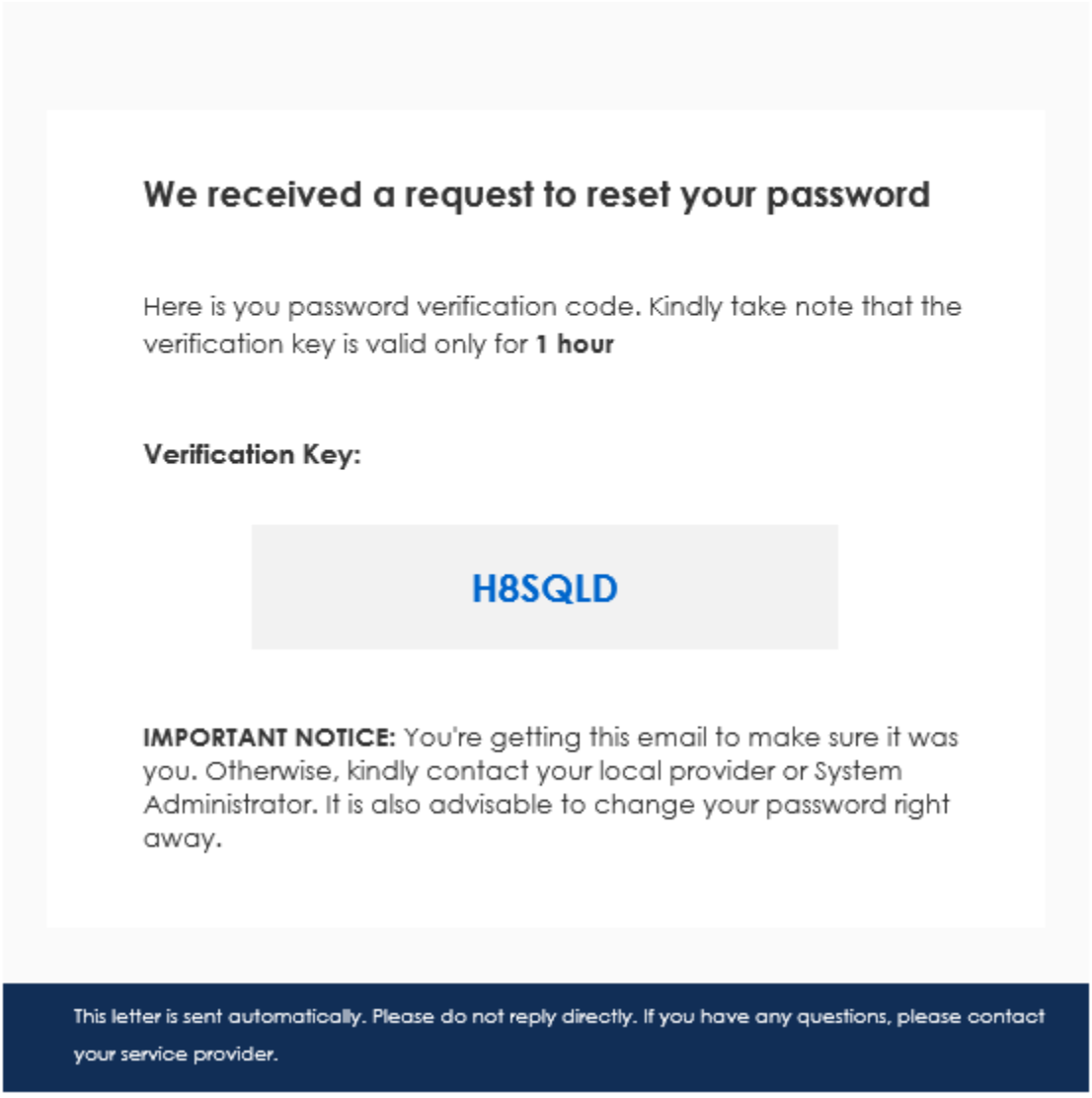


FIGURE 2.5 Face Manager password reset email code

7. Go back to the Face Manager server and enter the verification code from the email, click "Next", if you didn't receive the password reset email then click "Resend Verification Code" and wait for the password reset email

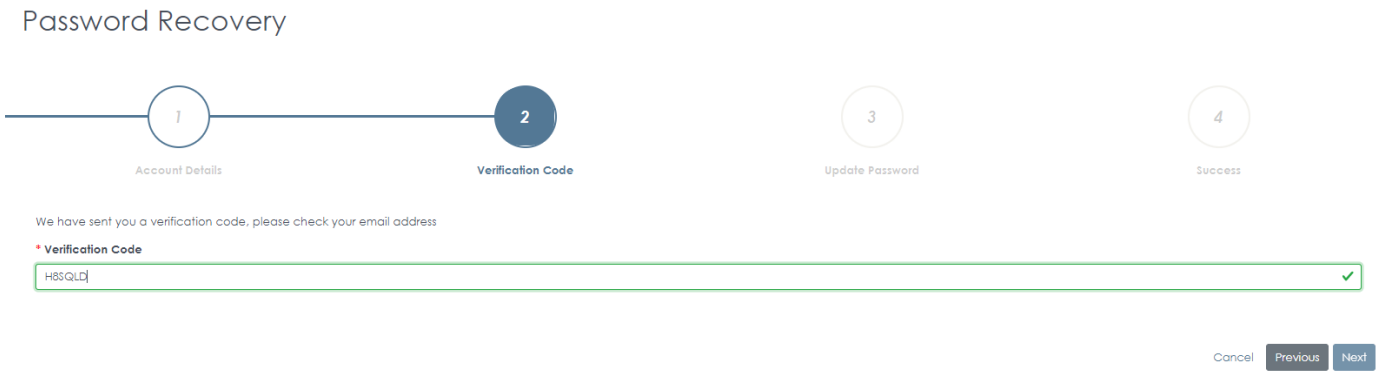


FIGURE 2.6 Face Manager password reset email code

8. If the verification code is correct, the user will be prompted to enter a new password, click "Next".

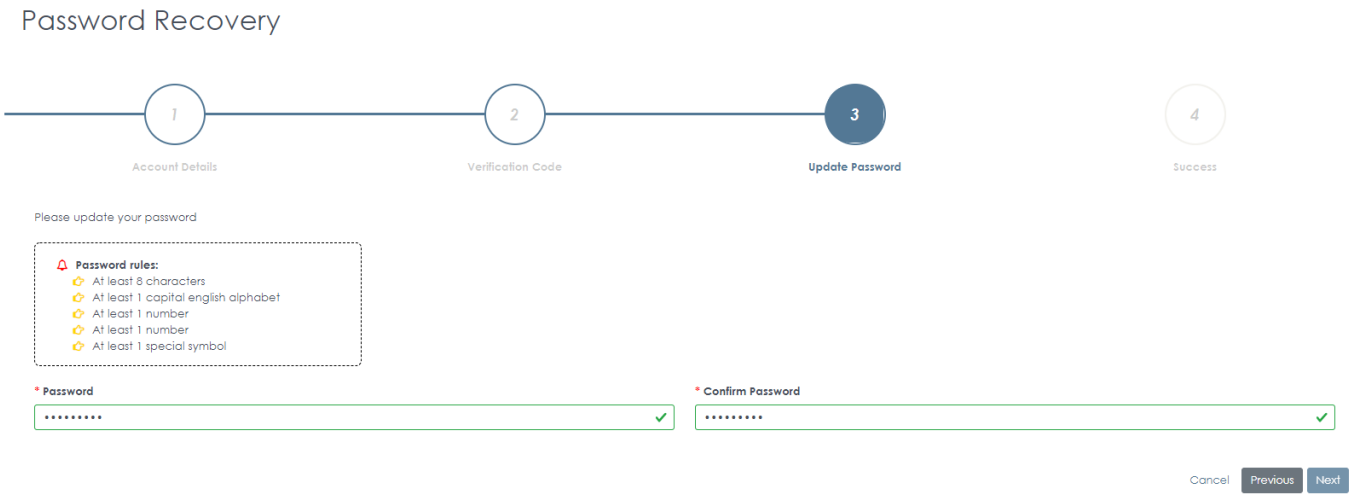


FIGURE 2.7 Face Manager setup new password

9. A confirmation message will be displayed to inform the user that the password for the account has been successfully reset.

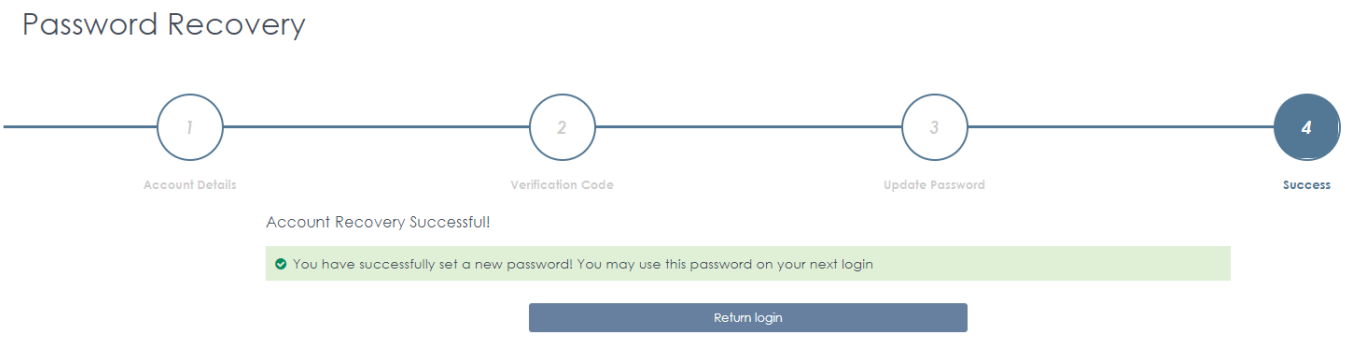


FIGURE 2.8 Face Manager reset success

10. Login to Face Manager with the new password

2.2 Investigation Report

2.2.1 Real-time monitoring report

Remark

- This type of report (also known as "instant result report") is used to instantly display face recognition events for the purpose of immediately verifying a person's identity for possible applications such as: security guards, concierges, or service desks

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with Administrator credentials
3. Navigate to "Investigation" menu ➡"Monitoring"

Remark

- By default, this report does not show face recognition events, only new events

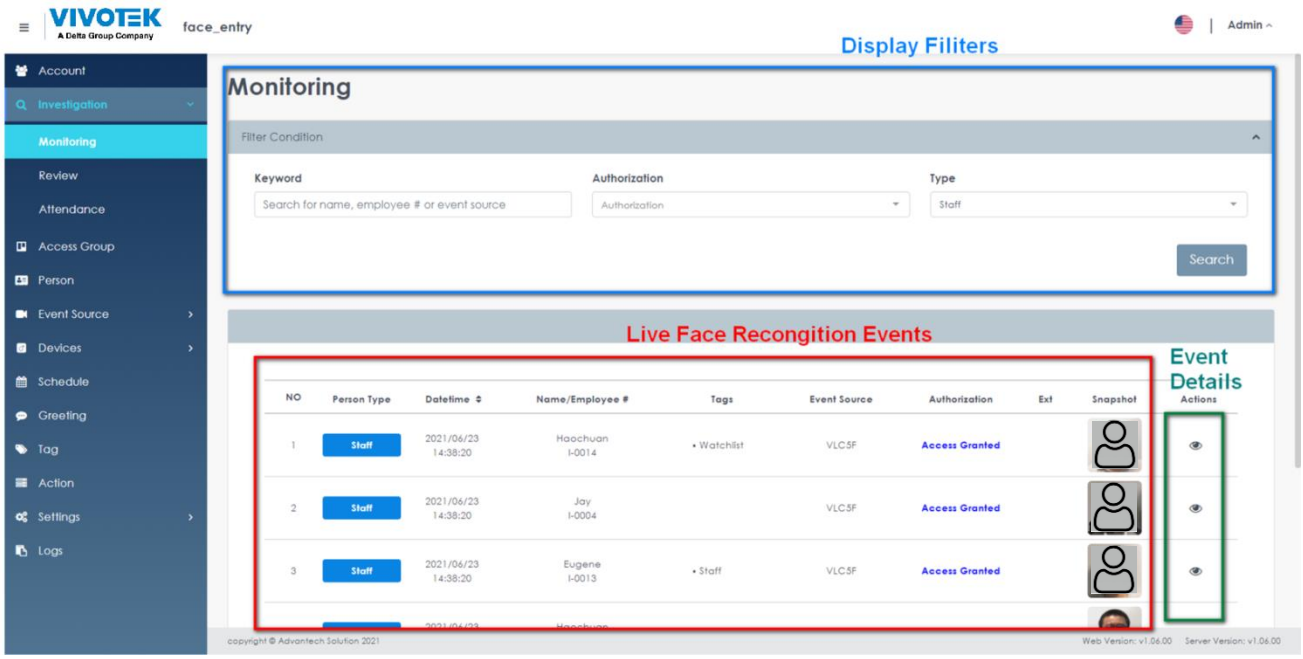


FIGURE 2.9 Face Manager Monitoring Report

4. Use filters to narrow the results by name, person type or authorization
5. Click the "Filter" button
6. Only events that meet the filter criteria will be displayed on the screen
7. To view the full details of Face Recognition events, click on the "Event Details" icon

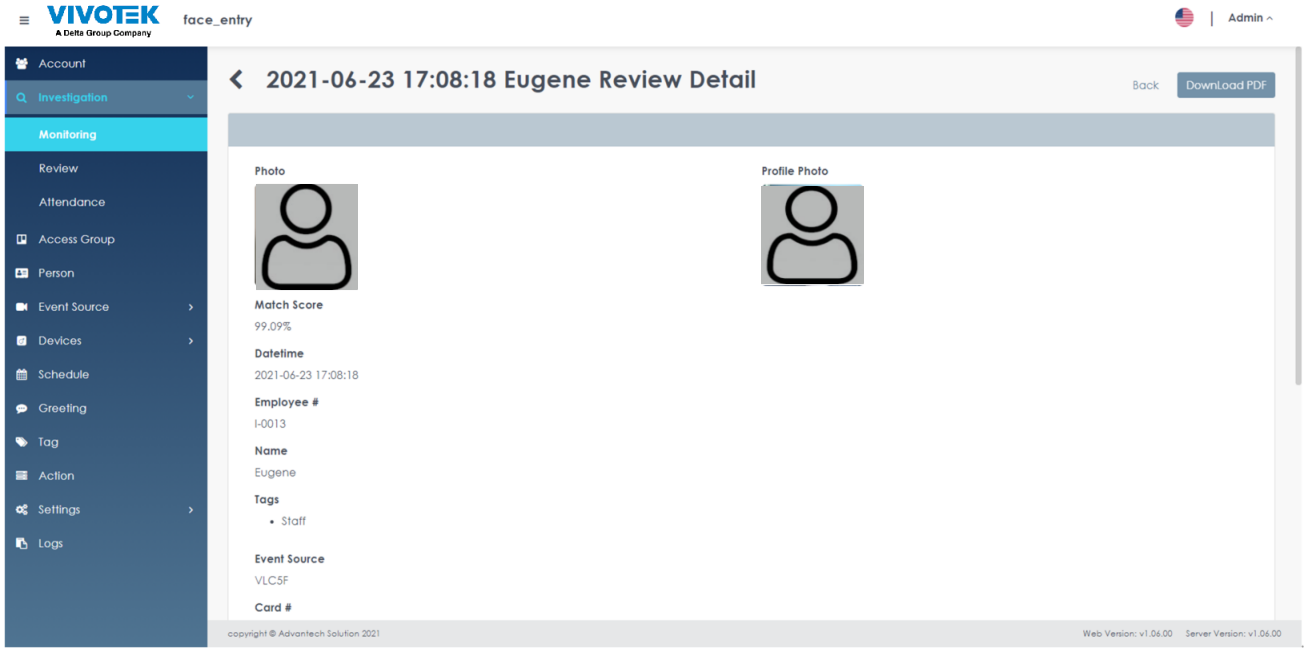


FIGURE 2.10 Face Manager Monitoring Report Event Details

8. If you need to export events, click on the "Export to PDF" button, which will export all the full details of the Face Recognition event to a .PDF file

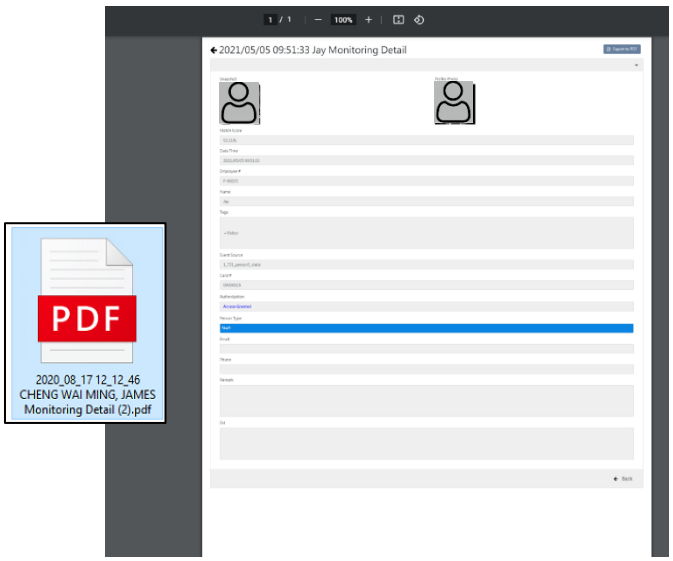


FIGURE 2.11 Face Manager Monitoring Report Export to PDF

2.2.2 Historical Records

Remark

- This type of report (also known as a "history report") is used to display past face recognition events with the goal of providing a reliable log of face recognition event access

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with Administrator credentials
3. Navigate to "Investigation" menu ➡"Review"

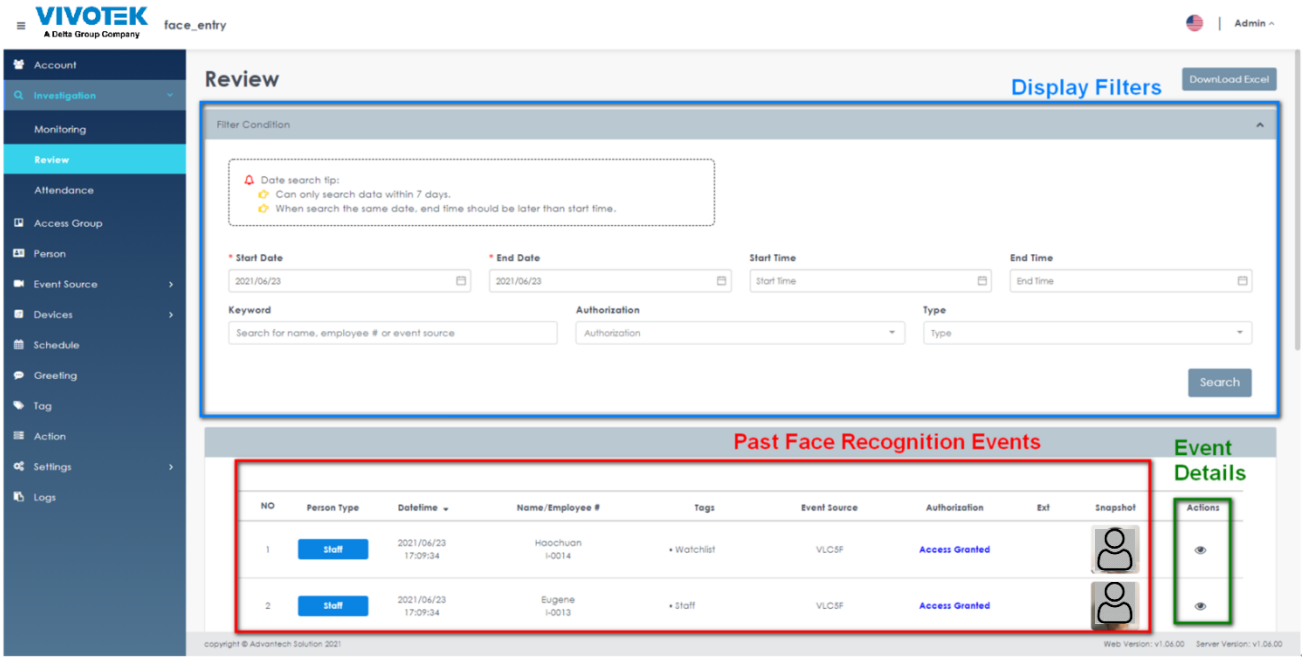


FIGURE 2.12 Face Manager Review Report

4. Use filters to narrow down results by name, person type, authorization or date range
5. Click the "Search" button
6. Only events that meet the filter criteria will be displayed on the screen
7. To view the full details of the Face Recognition event, click on the "Event Details" icon (⋮) and select "View"

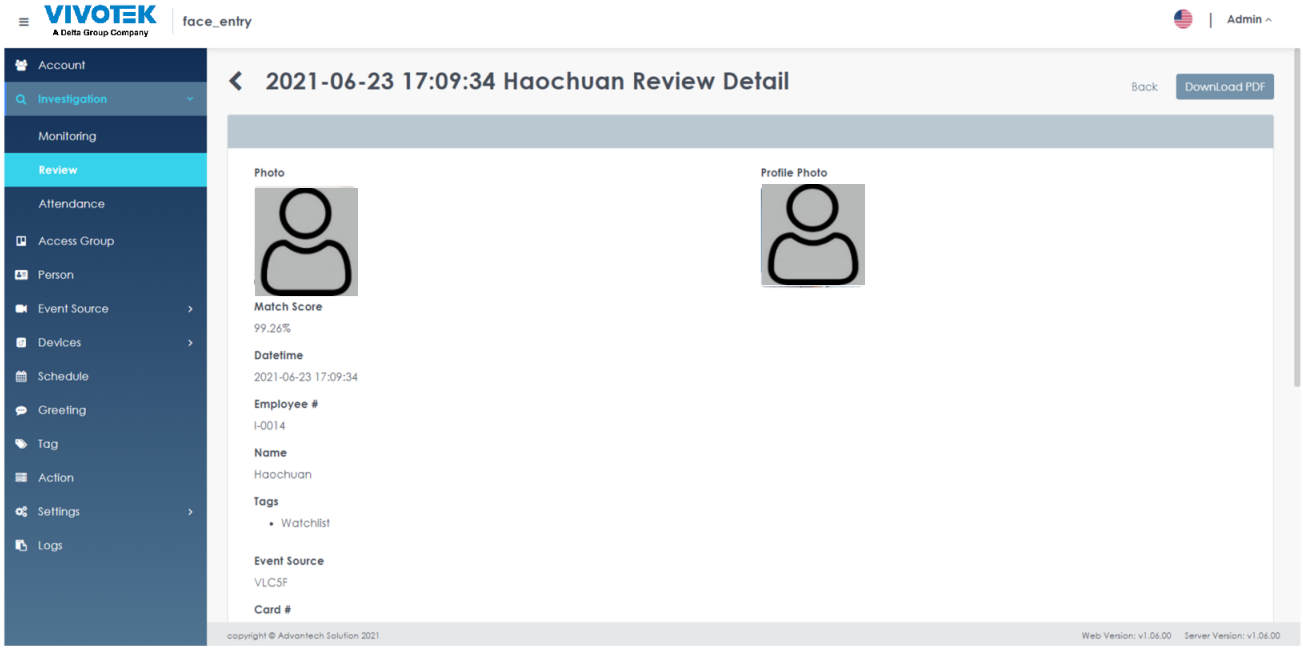


FIGURE 2.13 Face Manager Review Report Event Details

8. If you need to export events, click on the "Export to PDF" button, which will export all the full details of the Face Recognition event to a .PDF file

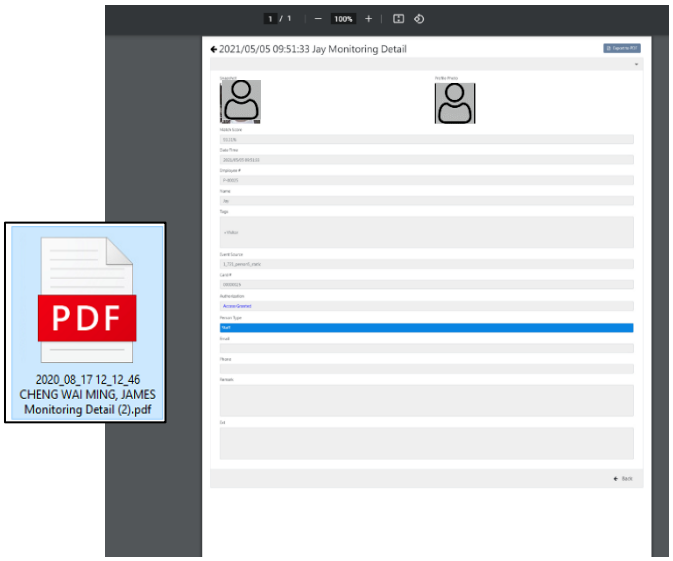
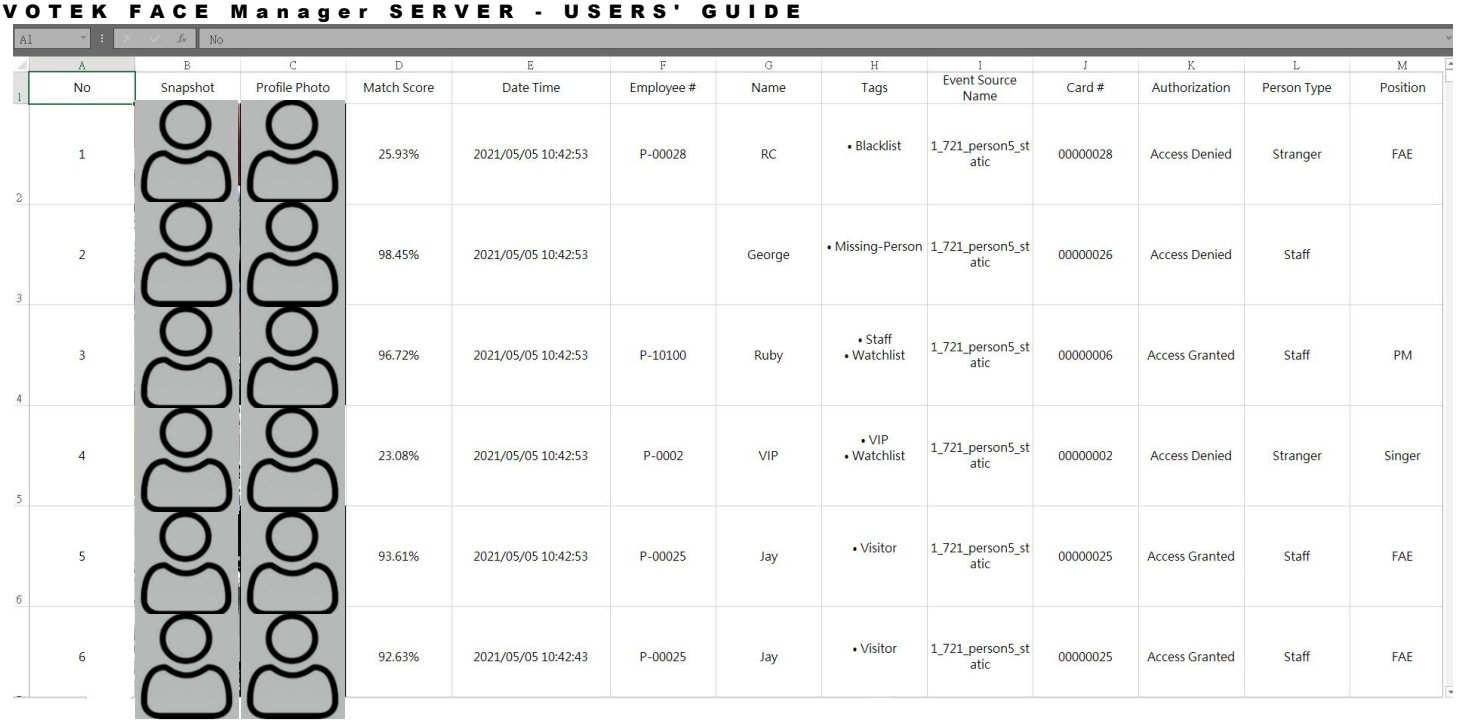


FIGURE 2.14 Face Manager Review Report Export to PDF

9. To export all FR events on the screen to an Excel file, click the "Export to Excel" button

10.



No	Snapshot	Profile Photo	Match Score	Date Time	Employee #	Name	Tags	Event Source Name	Card #	Authorization	Person Type	Position
1			25.93%	2021/05/05 10:42:53	P-00028	RC	• Blacklist	1_721_person5_static	00000028	Access Denied	Stranger	FAE
2			98.45%	2021/05/05 10:42:53		George	• Missing-Person	1_721_person5_static	00000026	Access Denied	Staff	
3			96.72%	2021/05/05 10:42:53	P-10100	Ruby	• Staff • Watchlist	1_721_person5_static	00000006	Access Granted	Staff	PM
4			23.08%	2021/05/05 10:42:53	P-0002	VIP	• VIP • Watchlist	1_721_person5_static	00000002	Access Denied	Stranger	Singer
5			93.61%	2021/05/05 10:42:53	P-00025	Jay	• Visitor	1_721_person5_static	00000025	Access Granted	Staff	FAE
6			92.63%	2021/05/05 10:42:43	P-00025	Jay	• Visitor	1_721_person5_static	00000025	Access Granted	Staff	FAE

FIGURE 2.15 Face Manager Review Report Export to Excel

2.2.3 Access control

Remark

- This type of report (also known as an "Attendance Report") is used to show when registered personnel enter/leave the premises, possible applications include: security personnel, shift supervisors or personnel managers
- In addition, the gate entry/exit report requires face recognition equipment at each gate direction (entry and exit) to verify whether the person is arriving or departing the station. Dwell time is calculated as the time difference between the exit event minus the entry event

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with Administrator credentials
3. Navigate to "Investigation" menu " ➡ "Attendance Report"

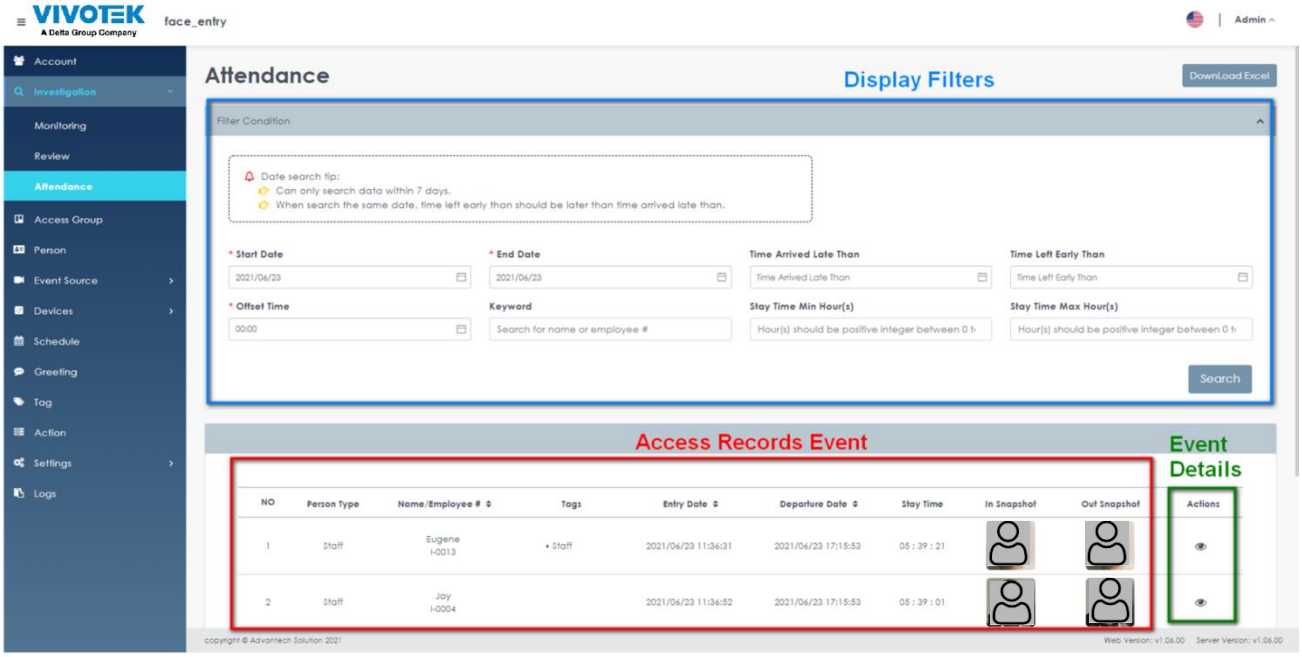


FIGURE 2.16 Face Manager Review Report Export to Excel

4. Use filters to narrow down results by name, stay time or date range
5. Click the "Search" button
6. Only events that meet the filter criteria will be displayed on the screen
7. To view the full details of the Face Recognition event, click on the "Event Details" icon (⋮) and select "View"

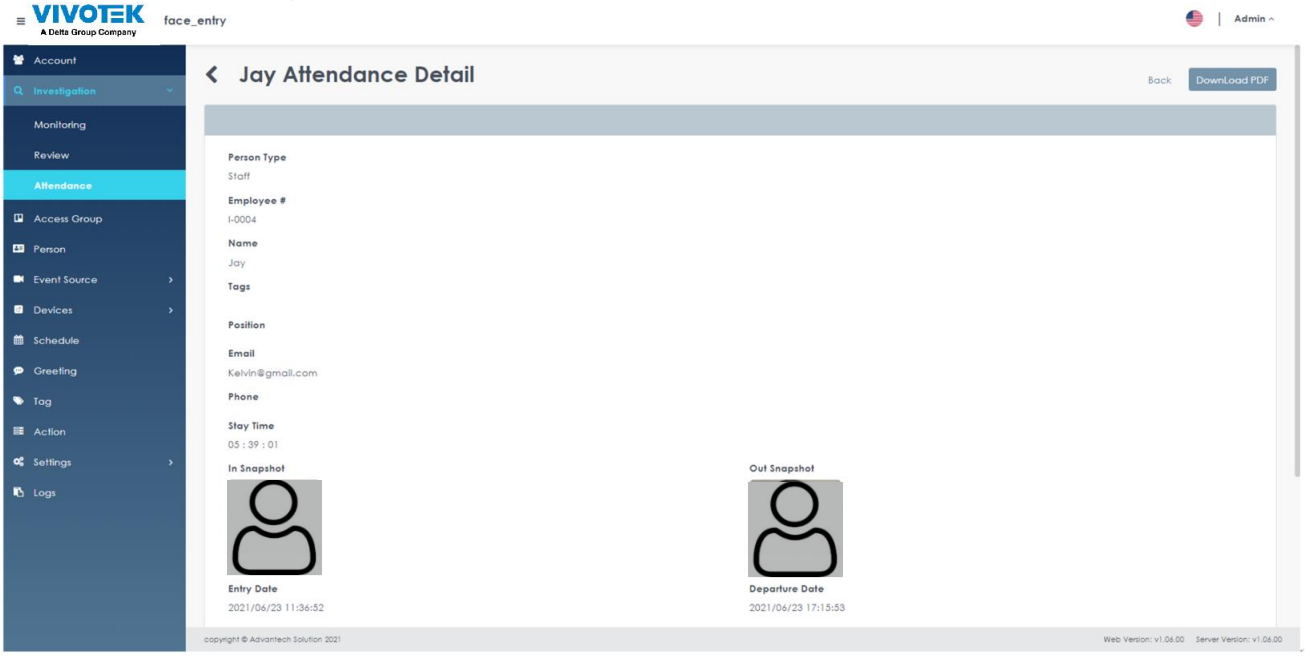


FIGURE 2.17 Face Manager Access Report Event Details

8. If you need to export events, click on the "Export to PDF" button, which will export all the full details of the Face Recognition events to a .PDF file

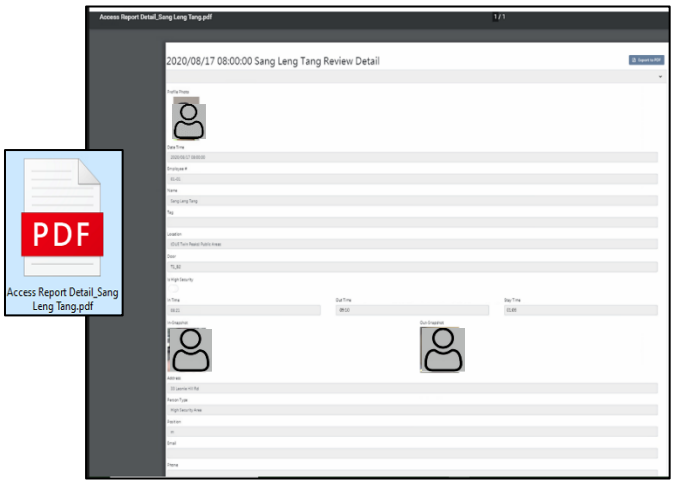


FIGURE 2.18 Face Manager Access Report Export to PDF

9. To export all FR events on the screen to an Excel file, click the "Export to Excel" button

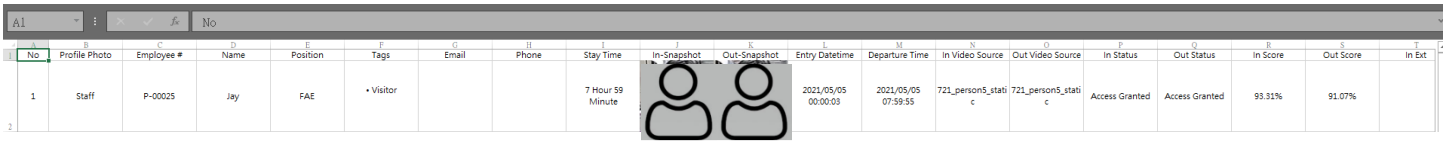


FIGURE 2.19 Face Manager Review Report Export to Excel

2.3 Group Management

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with Administrator credentials
3. Navigate to "Access Group" in the menu, which will display a list of the groups that have been set up for area access

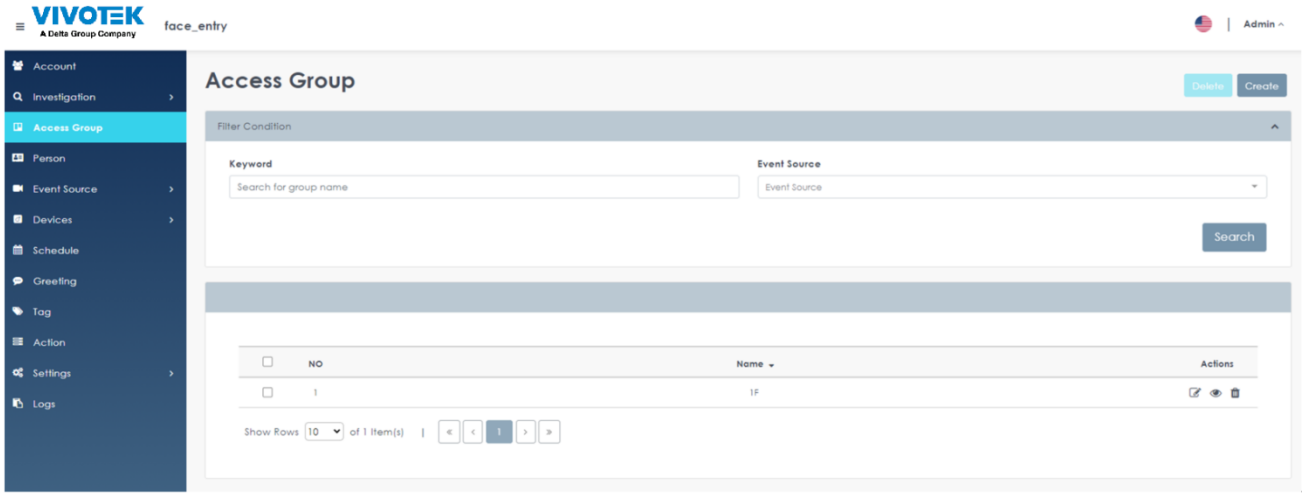


FIGURE 2.20 Face Manager Access Area Group

4. Use filters to narrow down results by group name or event source
5. Click the "Search" button
6. Only groups that meet the filter criteria will be displayed on the screen
7. To view the full details of the group, click on the "Event details" icon (⋮) and select "View"

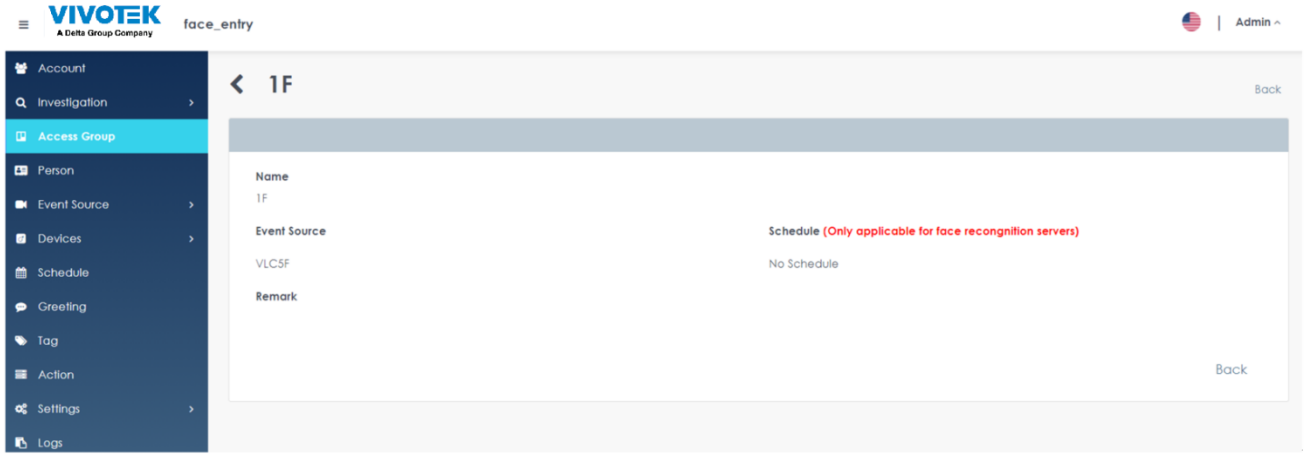


FIGURE 2.21 Face Manager Access Report details

8. To edit the group details, click on the "Event details" icon (⋮) and select "Modify"

9. Modify content according to requirements

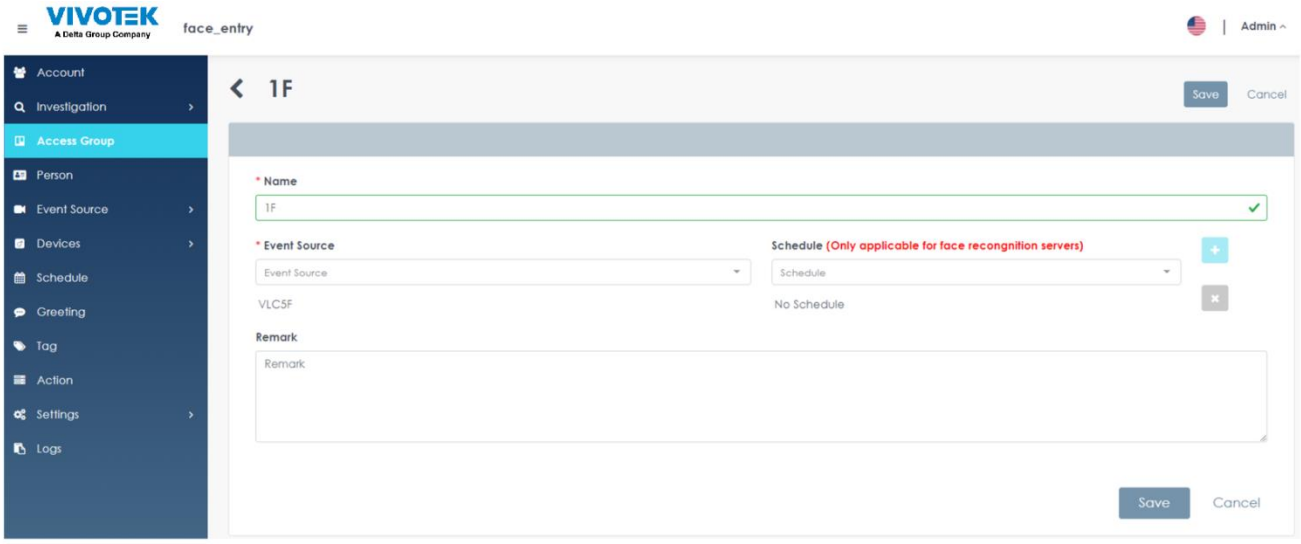


FIGURE 2.22 Face Manager Access Report Edit

10. Click Save to apply changes
11. To delete data, click on the "Event Details" icon (⋮) and select "Delete".
12. A pop-up window will appear on the screen, prompting the user to confirm the action

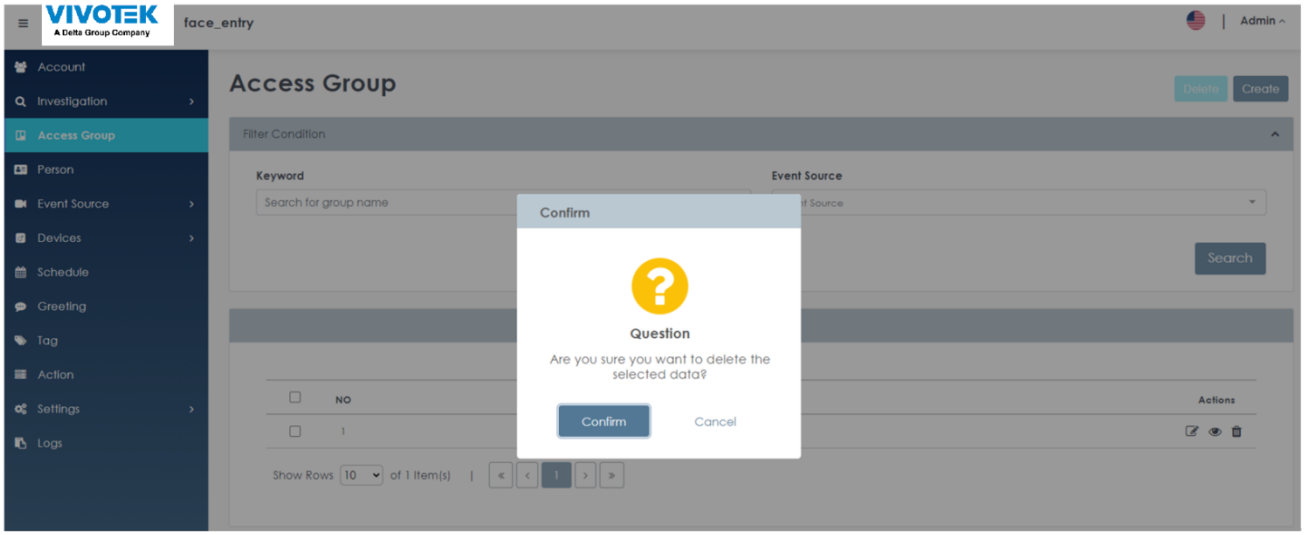


FIGURE 2.23 Face Manager Access Report Delete

13. Click "Confirm" to delete the selected group data
14. To add a new group, click the "+ Create" button

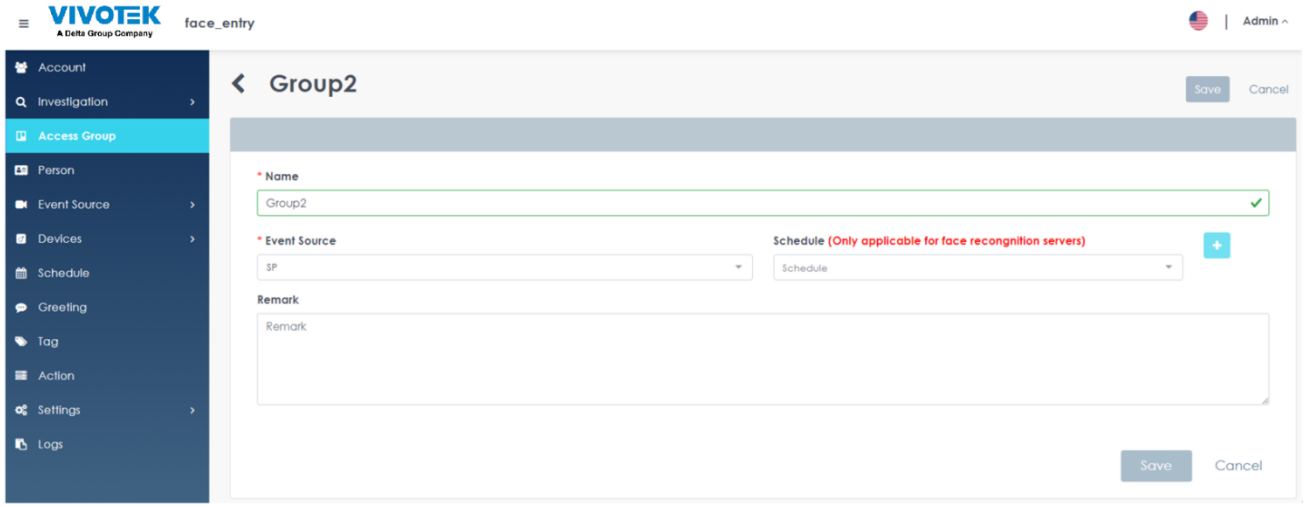


FIGURE 2.24 Face Manager Access Report Create

15. On the "Create Group" menu, enter data for the new:
    a. Group Name ➡ Enter a custom group name
    b. Image Source Name ➡ Select Image Source
    c. Scheduling ➡ Select the scheduling rules to be set (multiple groups can be set, please click the + sign in the upper right corner to add new settings after selection)
    d. Remarks ➡ (optional) You can enter your own description for this group
16. Click "Save" to create group data

2.4 Face Manager People Data Management

2.4.1 Face Data Management

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with Administrator credentials
3. Navigate to "Person" in the menu, which will display a list of all people who have registered their face information

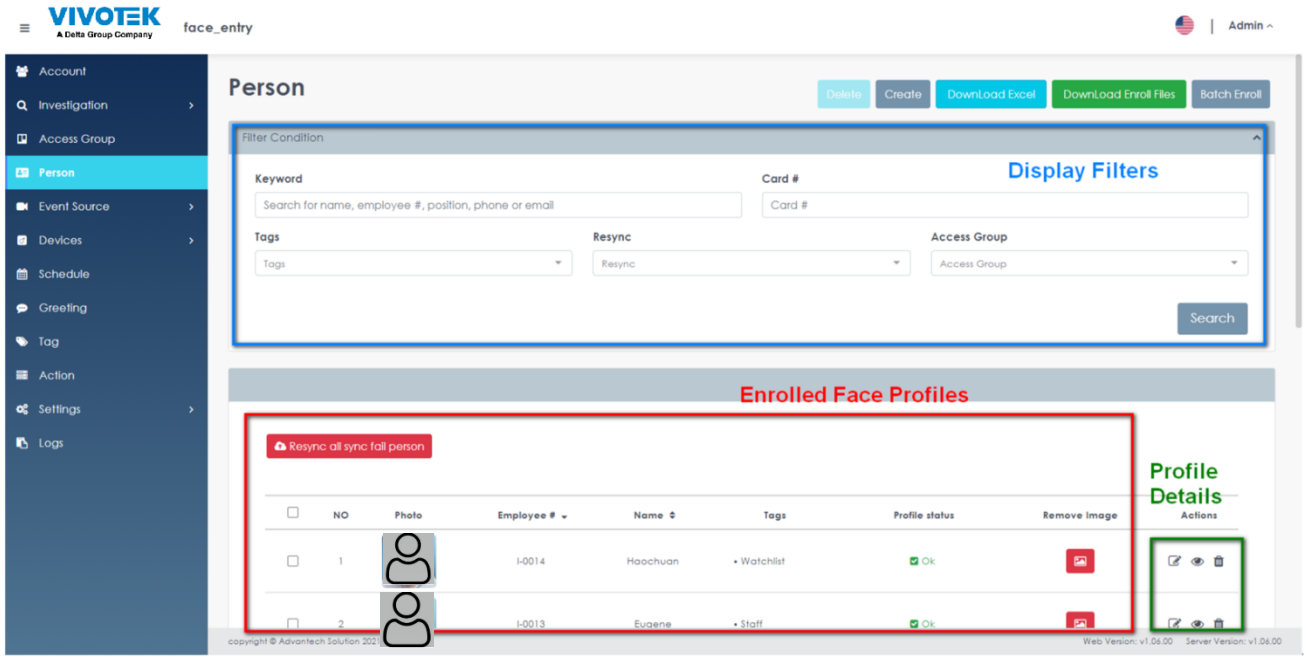


FIGURE 2.25 Face Manager enrolled face profiles

4. Use filters to narrow down results by name, tag, access group or card number
5. Click the "Search" button to display only the information that meets the filter criteria.
6. In order to view the details of a person's data, click on the "Details" ⋮ icon and select "Edit", which will display the full details of the selected data
7. Edit data as required

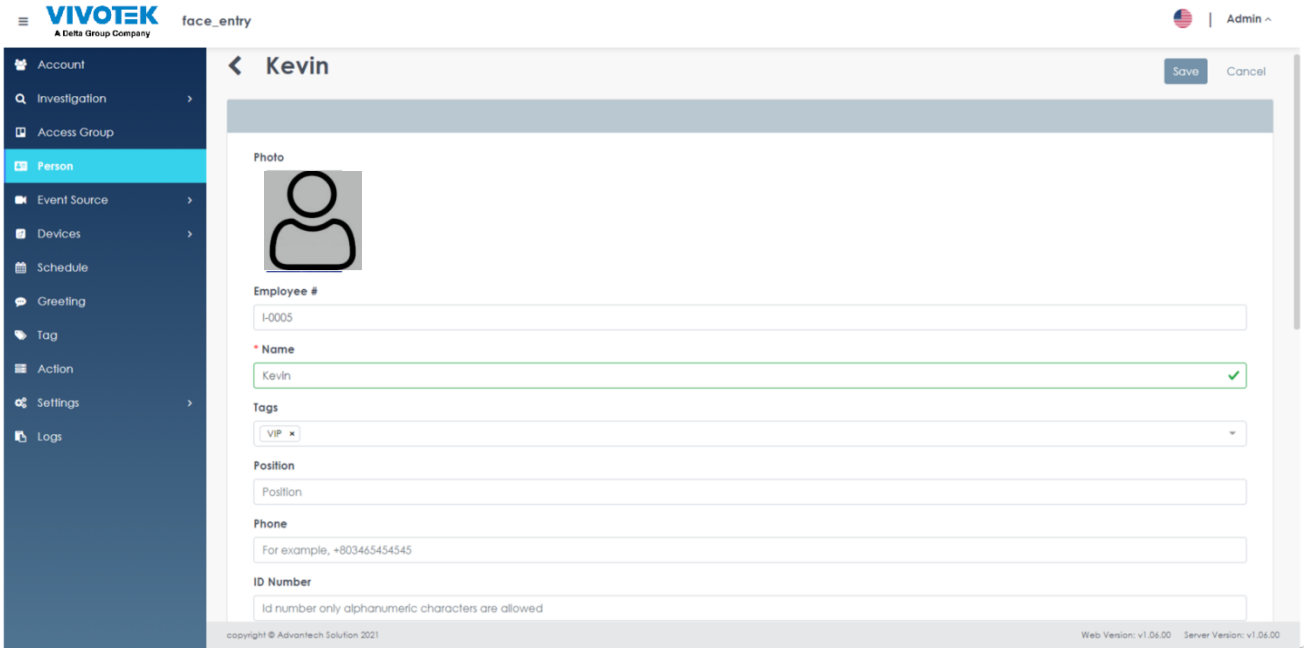


FIGURE 2.26 Face Manager face profile with full details

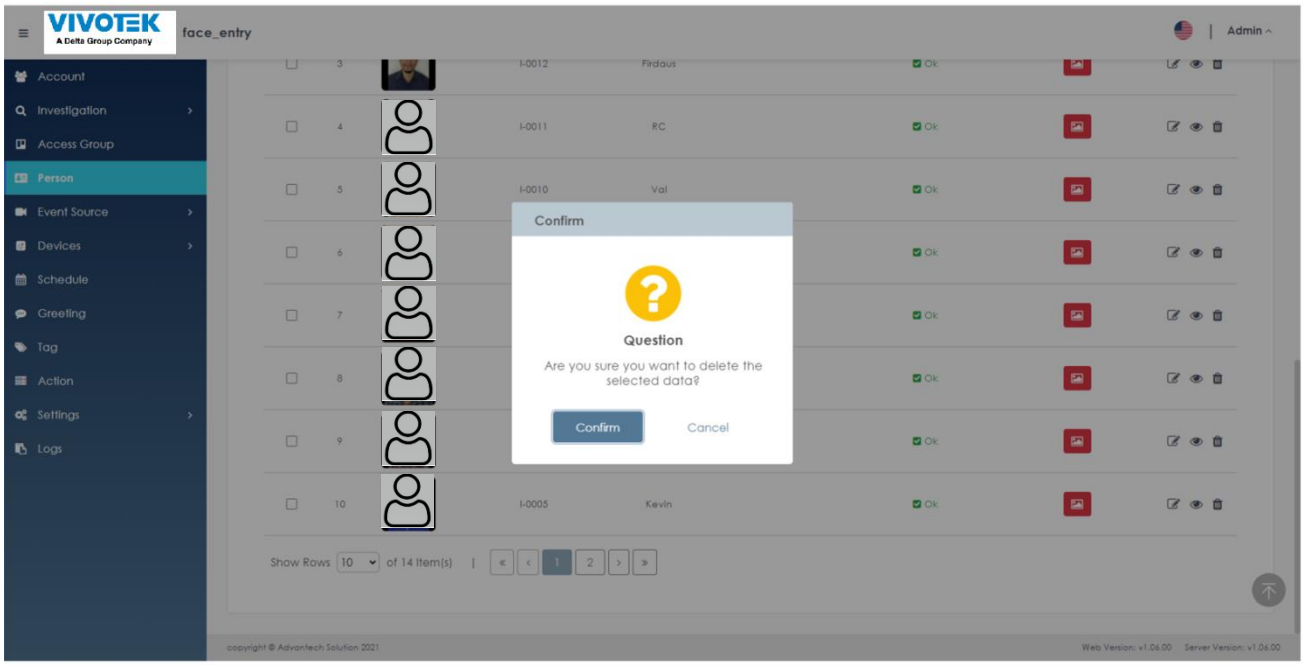
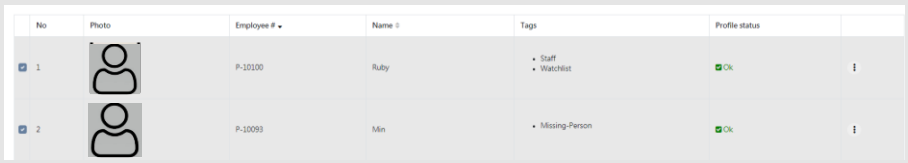
8. Click "Save" to apply changes
9. To delete data, click on the "Details" icon ⋮ and select Delete
10. A pop-up window will appear on the screen, prompting the user to confirm the action
11. 

FIGURE 2.27 Face Manager delete face profile

12. Click "Confirm" to delete the selected person's information

Remark

- If you need to delete more than one person's data at a time, on the leftmost column (to the left of the number), check the boxes to select persons and click on the delete icon ( )



13. To add personnel information, click the "+ Create" button (+ Create)
14. On the "Create Profile" menu, enter data for the new person:
    a. Photo ➡ Personal profile photo for face recognition (selected image must be .PNG, .JPG or .JPEG and must be less than 1 MB)
    b. Employee Number ➡ (optional)
    c. Name ➡ Name of person
    d. Tags ➡ (optional) Additional tags used to further classify this person
    e. Position ➡ (optional)
    f. Phone ➡ (optional)
    g. Identification (ID) ➡ (optional)
    h. Email ➡ (optional)
    i. Remark ➡(optional)
    j. Card Number➡ (Optional) The virtual card number to be assigned to this person's data.
    k. Access password➡ (optional) The password to be set for using the tablet
    l. **Expiration Date** ➡ The last approved date that a registered person can be authenticated on the Face Manager server, after which the person's data will be automatically deleted from the system
    m. Access Group ➡(optional) Select a group that has been set up

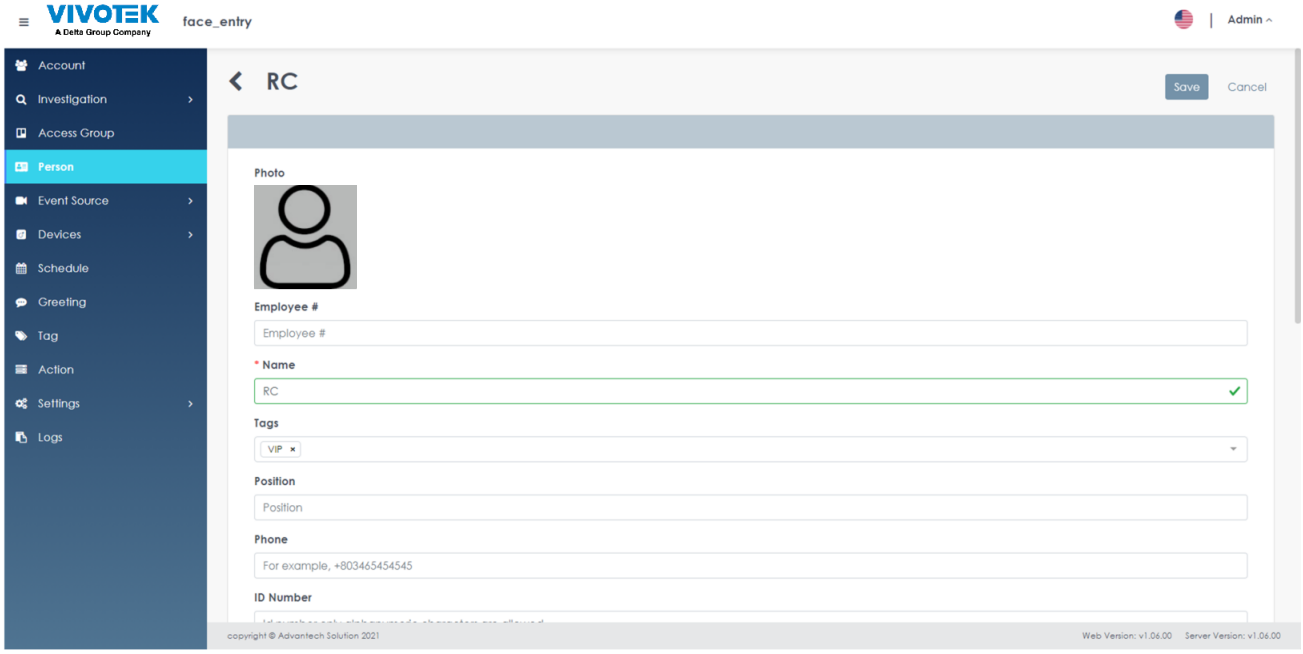


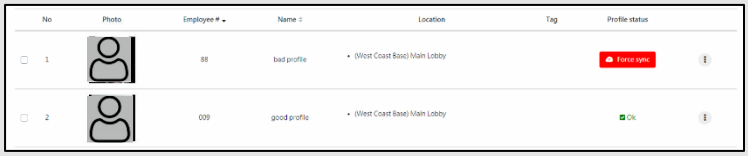
FIGURE 2.28 Face Manager Create face profile

15. Click "Save" to create a person

Remark

- After a new person is created, it will take some additional time for the Face Manager server to register it to all connected Face Recognition devices. The newly created face data will be marked as "not synchronized" until the process is successfully completed in all FR devices.

- If the synchronization process takes longer than usual, or if any Face Recognition device was unavailable at the time (i.e., FR device was offline), the user can click the (Force sync) button to try to register the person's data to all Face Recognition devices



2.4.2 Bulk enrollment

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with Administrator credentials
3. Navigate to "Person" in the menu, which will display a list of all people who have registered their face information
4. Click on the "Enroll" button to display the bulk enrollment page ( )

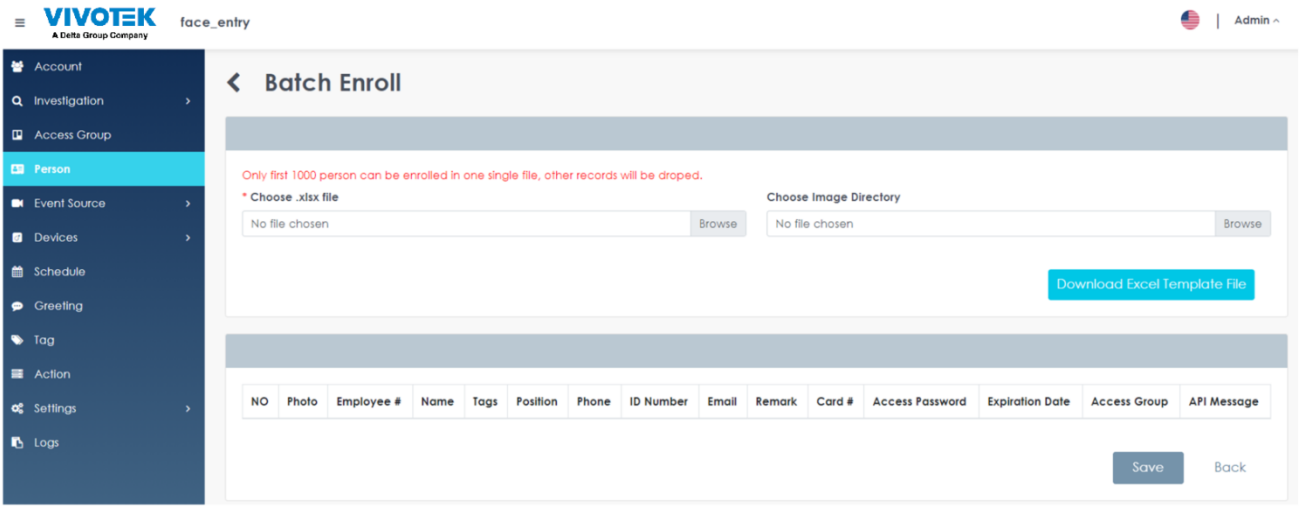


FIGURE 2.29 Face Manager Bulk Enrollment page

5. Click on "Download Excel template file"
6. On a PC with Microsoft Excel, open the example file, edit it as required and save all changes

No	Photo	Employee #	Name	Tag	Position	Phone	ID Number	Email	Remark	Card #	Access Password	Expiration Date	Access Group
1	坂本昌行.jpg	v6_1	坂本昌行	VIP;VIP	演員	+0139399688	v6001	v6_1@gmail.com	Love-v6x1	11223344	ssss	2025/02/05	;Company 3 - Group 3;Company 3 - Group 3
2	長野博.jpg	v6_2	長野博	Blacklist;Blacklist	偶像	+0633249806	v6002	v6_2@gmail.com	Like-v6x2	55667788	fgdfgd	2030/12/24	;Company 3 - Group 2;Company 3 - Group 2
3	井之原快彥.jpg	v6_3	井之原快彥	Missing-Person;VIP	歌手	+0242911905	v6003	v6_3@gmail.com	Heart-v6x3	99001122	fgjgyi	2035/09/19	;Company 3 - Group 3;Company 3 - Group 1
4	森田剛.jpg	v6_4	森田剛	Watchlist;Blacklist	演員	+0974919128	v6004	v6_4@gmail.com	Love-v6x100	33445566	tyhj	2040/08/18	;Company 3 - Group 2;Company 3 - Group 3
5	三宅健.jpg	v6_5	三宅健	VIP;VIP	偶像	+0592170395	v6005	v6_5@gmail.com	Like-v6x200	77889900	ddddddddd.	2045/11/11	;Company 3 - Group 3;Company 3 - Group 2
6	岡田准一.jpg	v6_6	岡田准一	Blacklist;Blacklist	歌手	+0704916221	v6006	v6_6@gmail.com	Heart-v6x300	9876543210	gjghjgj	2055/12/12	;Company 3 - Group 2;Company 3 - Group 1
7	坂本昌行.jpg	v6_1	坂本昌行	Missing-Person;VIP	演員	+0622827141	v6001	v6_1@gmail.com	Love-v6x1	11223344	ssss	2025/02/05	;Company 3 - Group 3;Company 3 - Group 3
8	長野博.jpg	v6_2	長野博	Watchlist;Blacklist	偶像	+0631430929	v6002	v6_2@gmail.com	Like-v6x2	55667788	fgdfgd	2030/12/24	;Company 3 - Group 2;Company 3 - Group 2
9	井之原快彥.jpg	v6_3	井之原快彥	VIP;VIP	歌手	+0814298502	v6003	v6_3@gmail.com	Heart-v6x3	99001122	fgjgyi	2035/09/19	;Company 3 - Group 3;Company 3 - Group 1
10	森田剛.jpg	v6_4	森田剛	Blacklist;Blacklist	演員	+0420560492	v6004	v6_4@gmail.com	Love-v6x100	33445566	tyhj	2040/08/18	;Company 3 - Group 2;Company 3 - Group 3
11	三宅健.jpg	v6_5	三宅健	Missing-Person;VIP	偶像	+0816795518	v6005	v6_5@gmail.com	Like-v6x200	77889900	ddddddddd.	2045/11/11	;Company 3 - Group 3;Company 3 - Group 2
12	岡田准一.jpg	v6_6	岡田准一	Watchlist;Blacklist	歌手	+0511402395	v6006	v6_6@gmail.com	Heart-v6x300	9876543210	gjghjgj	2055/12/12	;Company 3 - Group 2;Company 3 - Group 1
13	坂本昌行.jpg	v6_1	坂本昌行	VIP;VIP	演員	+0680442928	v6001	v6_1@gmail.com	Love-v6x1	11223344	ssss	2025/02/05	;Company 3 - Group 3;Company 3 - Group 3
14	長野博.jpg	v6_2	長野博	Blacklist;Blacklist	偶像	+0821498870	v6002	v6_2@gmail.com	Like-v6x2	55667788	fgdfgd	2030/12/24	;Company 3 - Group 2;Company 3 - Group 2
15	井之原快彥.jpg	v6_3	井之原快彥	Missing-Person;VIP	歌手	+0348025697	v6003	v6_3@gmail.com	Heart-v6x3	99001122	fgjgyi	2035/09/19	;Company 3 - Group 3;Company 3 - Group 1
16	森田剛.jpg	v6_4	森田剛	Watchlist;Blacklist	演員	+0510661961	v6004	v6_4@gmail.com	Love-v6x100	33445566	tyhj	2040/08/18	;Company 3 - Group 2;Company 3 - Group 3
17	三宅健.jpg	v6_5	三宅健	VIP;VIP	偶像	+0590597424	v6005	v6_5@gmail.com	Like-v6x200	77889900	ddddddddd.	2045/11/11	;Company 3 - Group 3;Company 3 - Group 2
18	岡田准一.jpg	v6_6	岡田准一	Blacklist;Blacklist	歌手	+0910903690	v6006	v6_6@gmail.com	Heart-v6x300	9876543210	gjghjgj	2055/12/12	;Company 3 - Group 2;Company 3 - Group 1

FIGURE 2.30 Face Manager Bulk Enrollment template file (Mandatory fields are highlighted in yellow)

7. Return to the Face Manager server, click on "Choose .xlsx file" and browse to select the edited excel file
8. Click "Choose image directory" and browse to select the folder where the person images are located
9. If there are some data validation errors in the file, Face Manager will mark the cell where the data needs to be modified, please note that all errors must be corrected before the person data can be created.

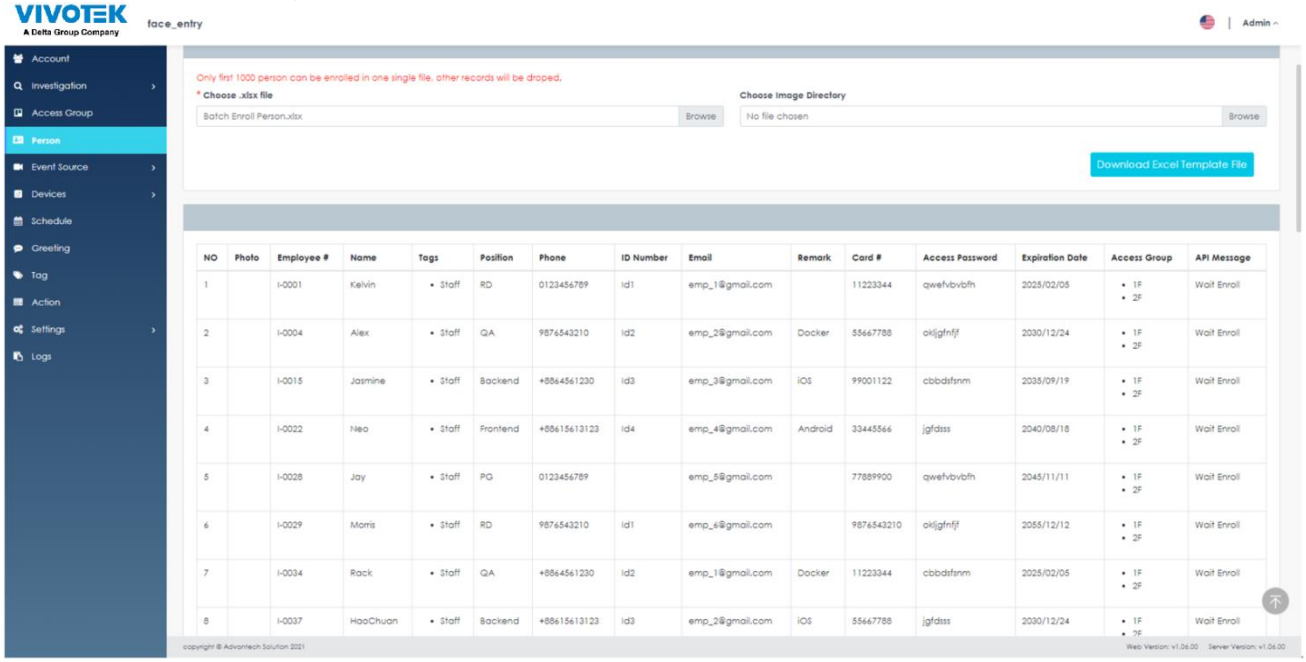


FIGURE 2.31 Face Manager Bulk Enrollment file and images showing an error

10. Once the file is correct, upload it again, click "Save", and wait for the person data to be created.
11. Once the person data is created, the system will display the bulk enrollment results

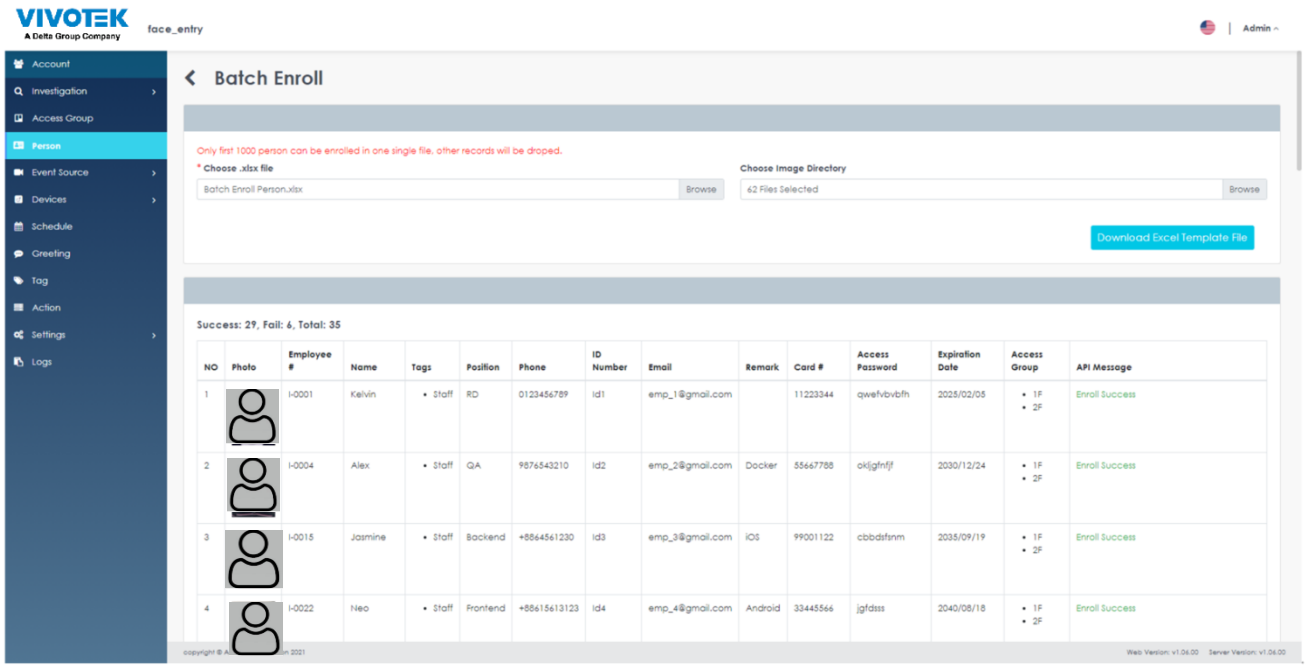


FIGURE 2.32 Face Manager Bulk Enrollment results

2.5 Scheduling Management

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with Administrator credentials
3. Navigate to "Schedule" in the menu, which will display a list of all set schedules

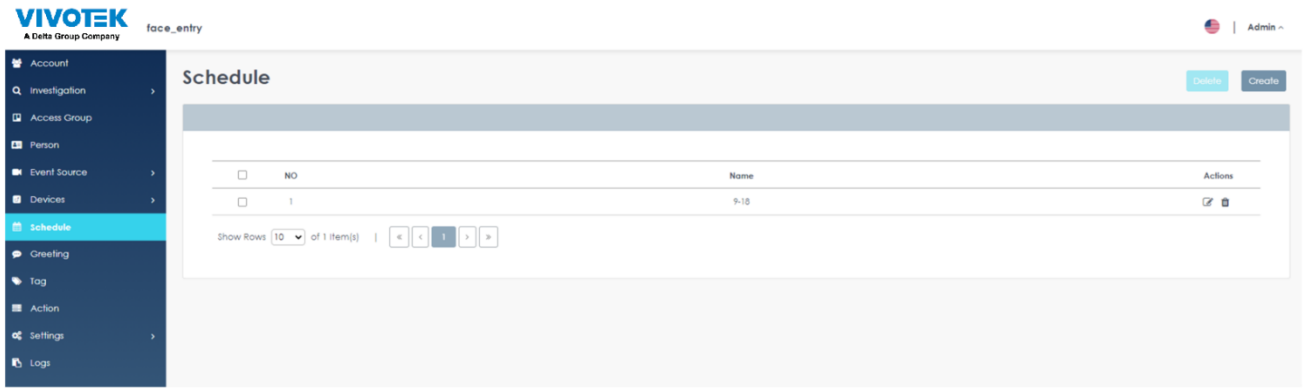


FIGURE 2.33 Face Manager Schedule List

4. In order to view the schedule details, click on the "Details" ⋮ icon and select "Edit", which will display the full details of the selected data
5. Edit related data as required

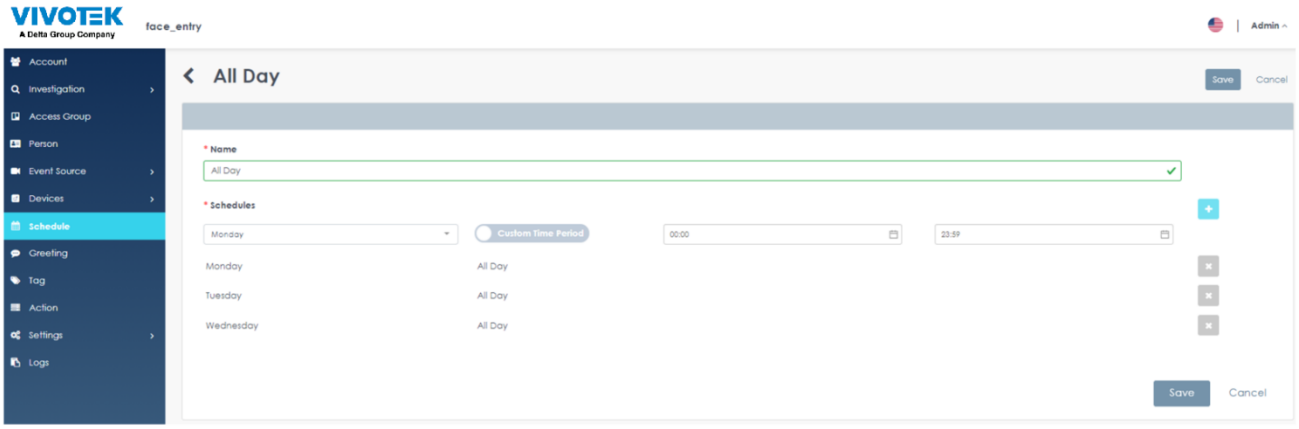


FIGURE 2.34 Face Manager Schedule Details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon ⋮ and select Delete
8. A pop-up window will appear on the screen, prompting the user to confirm the action

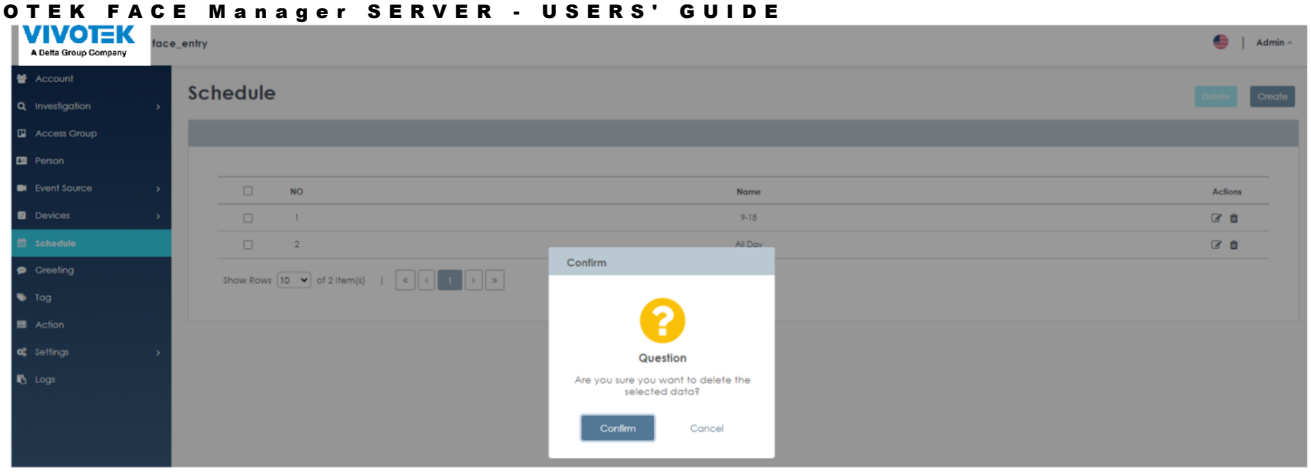


FIGURE 2.35 Face Manager Schedule Delete

9. Click "Confirm" to delete the selected scheduling data
10. To add scheduling data, click the "+ Create" button (+ Create)
11. On the "Create Schedule" menu, enter data for the new schedule.
    a. Name ➡ Custom name for the schedule
    b. Schedules➡Set the schedule and custom time period (multiple sets can be set)

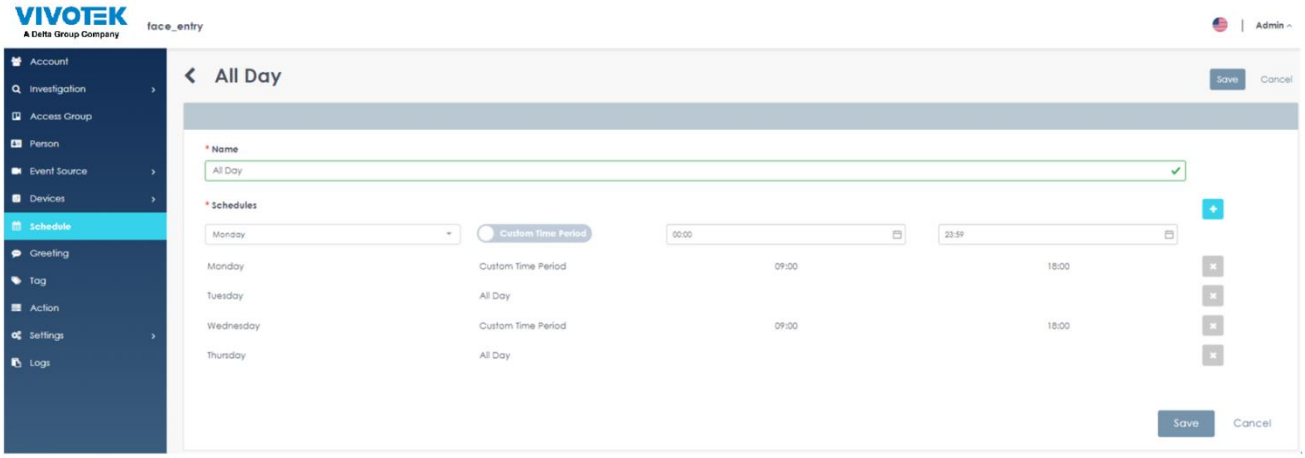


FIGURE 2.36 Face Manager Schedule Create

12. Click "Save" to create a schedule

2.6 Greeting Management

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with Administrator credentials
3. Navigate to "Greetings" in the menu, which will display a list of all the greetings that have been set

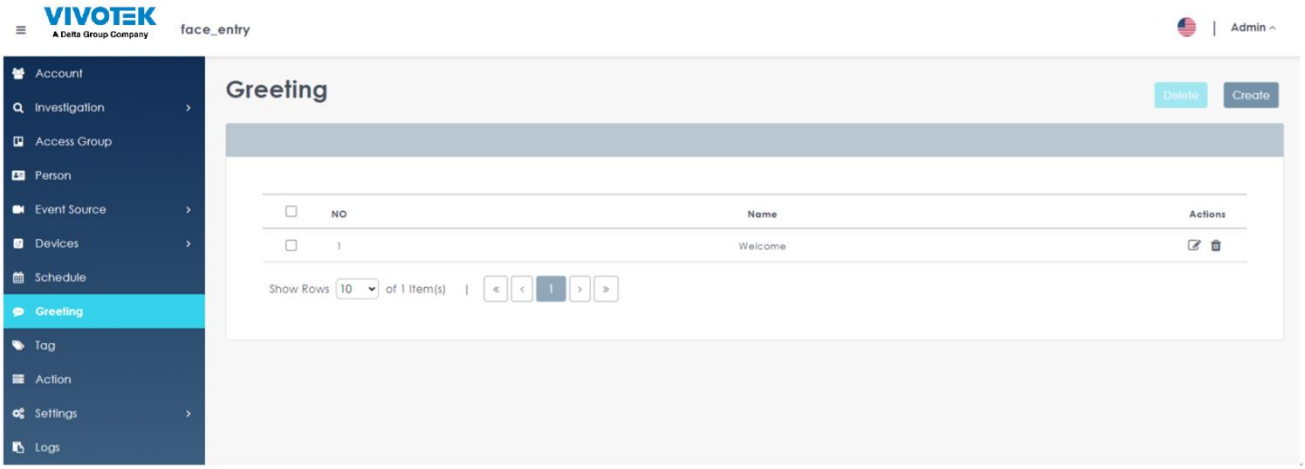


FIGURE 2.37 Face Manager Greeting List

4. To view the details of the greeting, click on the "Details" icon and select "Edit", which will display the full details of the selected data
5. Edit related data as required

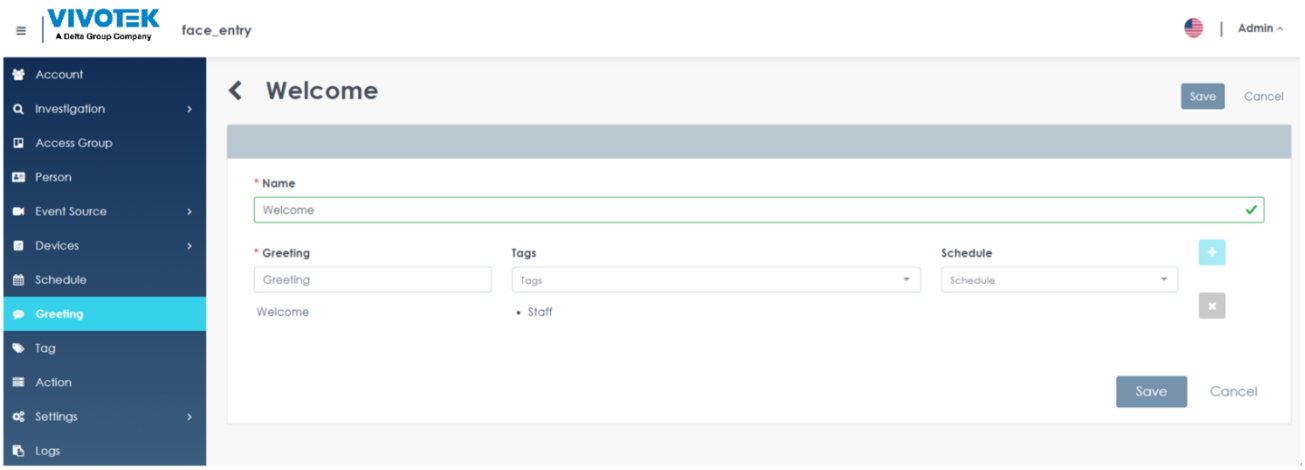


FIGURE 2.38 Face Manager Greeting Details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon and select Delete
8. A pop-up window will appear on the screen, prompting the user to confirm the action

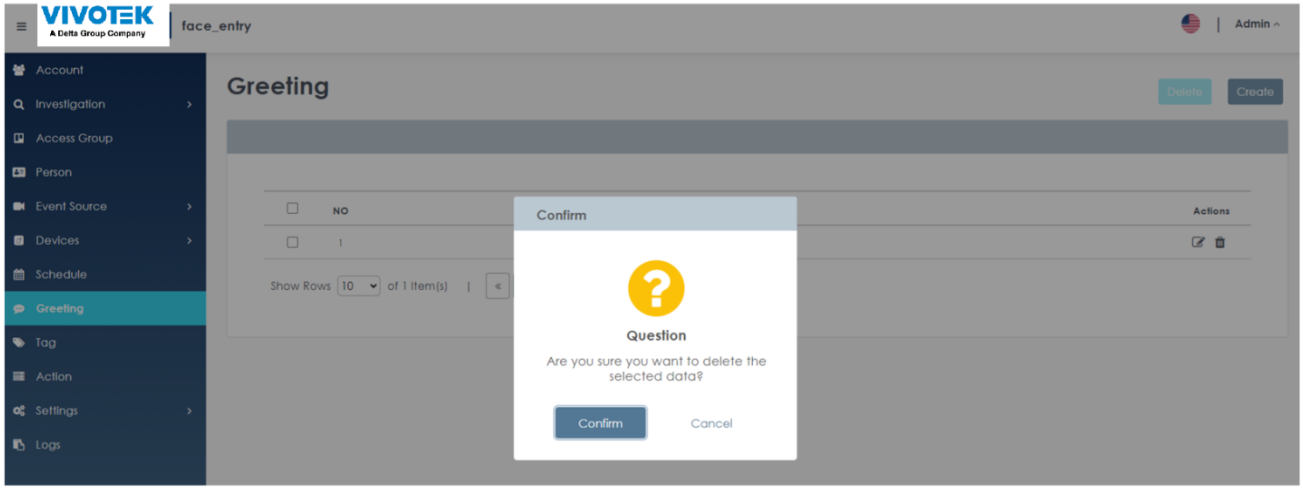


FIGURE 2.39 Face Manager Greeting Delete

9. Click "Confirm" to delete the selected scheduling data
10. To add greeting data, click the "+ Create" button (+ Create)
11. On the "Create greeting" menu, enter data for the new greeting:
    a. Name ➡ Custom greeting name
    b. Greetings ➡ Content of the greeting, applicable tags and custom scheduling (multiple sets can be set)

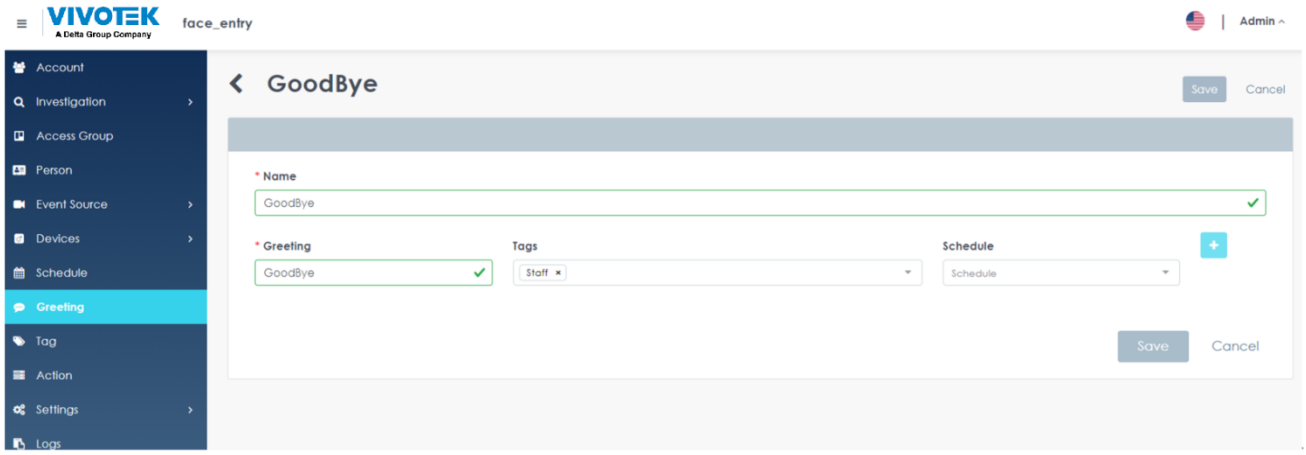


FIGURE 2.40 Face Manager Greeting Create

12. Click "Save" to create a greeting

2.7 Label Management

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login to Face Manager server with Administrator credentials

3. Navigate to "Tag" in the menu and click "+Create"

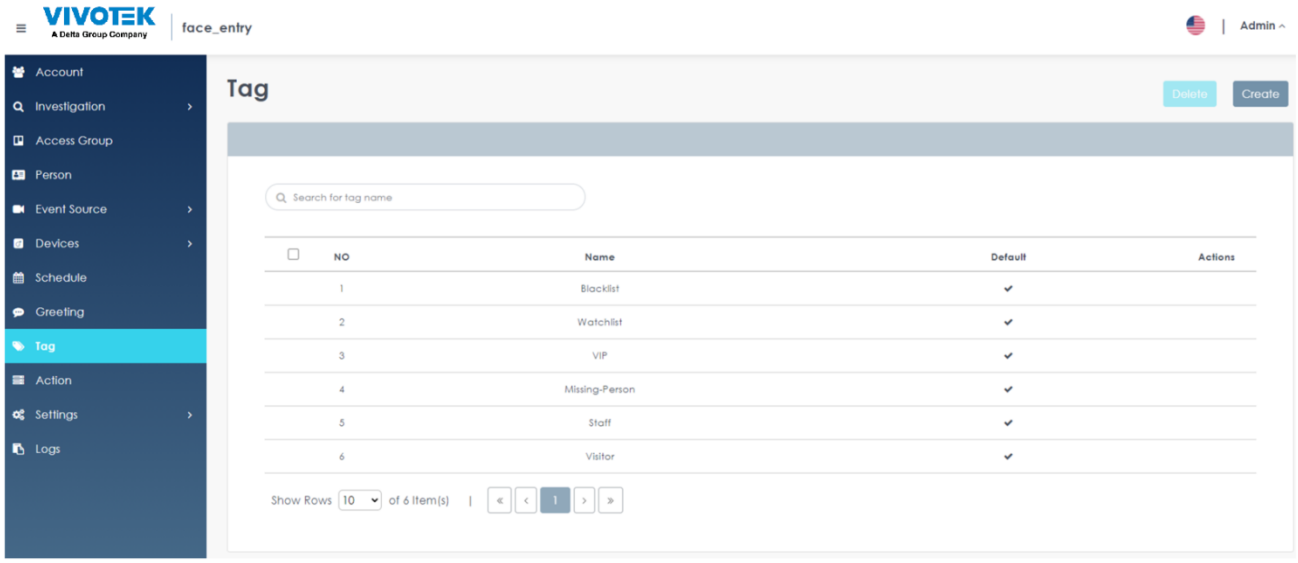


FIGURE 2.41 Face Manager Tag List

4. The "Create Tag" menu will be displayed

5. Enter a new tag name

6. Click "Save" to apply changes

Remark

- Tags provide a simple way to tag registered faces and provide additional information. Tags can be assigned based on organizational role (i.e. contractor, employee, part-time), assigned unit (i.e. IT, marketing, logistics) or any other form of logical grouping.

- Tags are universal and once created, they can be used by all Administrators in all companies for use on their assigned face data

2.8 Event Source Management (System Admin Only)

2.8.1 List of event sources

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Event Source" menu ➡ "Event Source List", which will display a list of all the image sources that have been set up

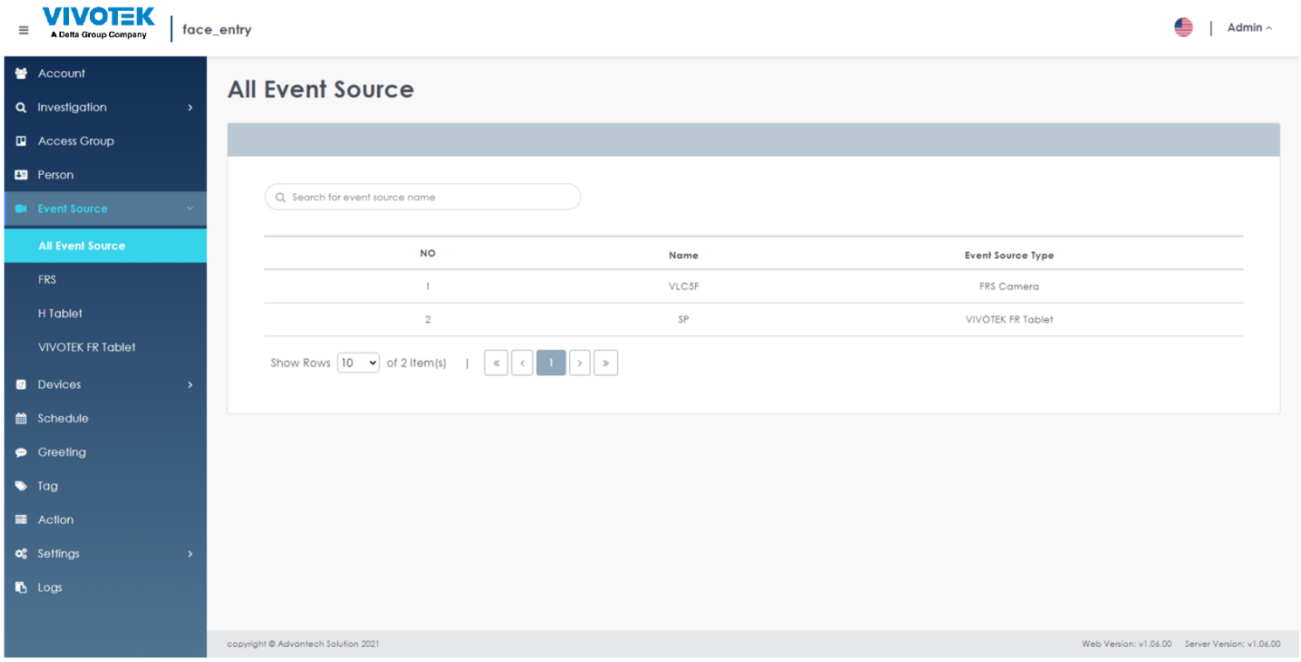


FIGURE 2.42 Face Manager Event Sources List

4. The list shows the following information:
    a. Number of licenses available ➡ Displays number of licenses currently in use/total licenses
    b. Event Source Name ➡ Custom image source name
    C. Source type ➡ Shows the type of image source (e.g. VAST Face Camera, H tablet...etc)
5. Use filters to narrow down results by event source name
6. Click the "Search" button to display only the information that meets the filter criteria.

2.8.2 VAST FACE

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to "Event Source" menu ➡ "VAST FACE", which will display a list of all the VAST FACE that have been set up

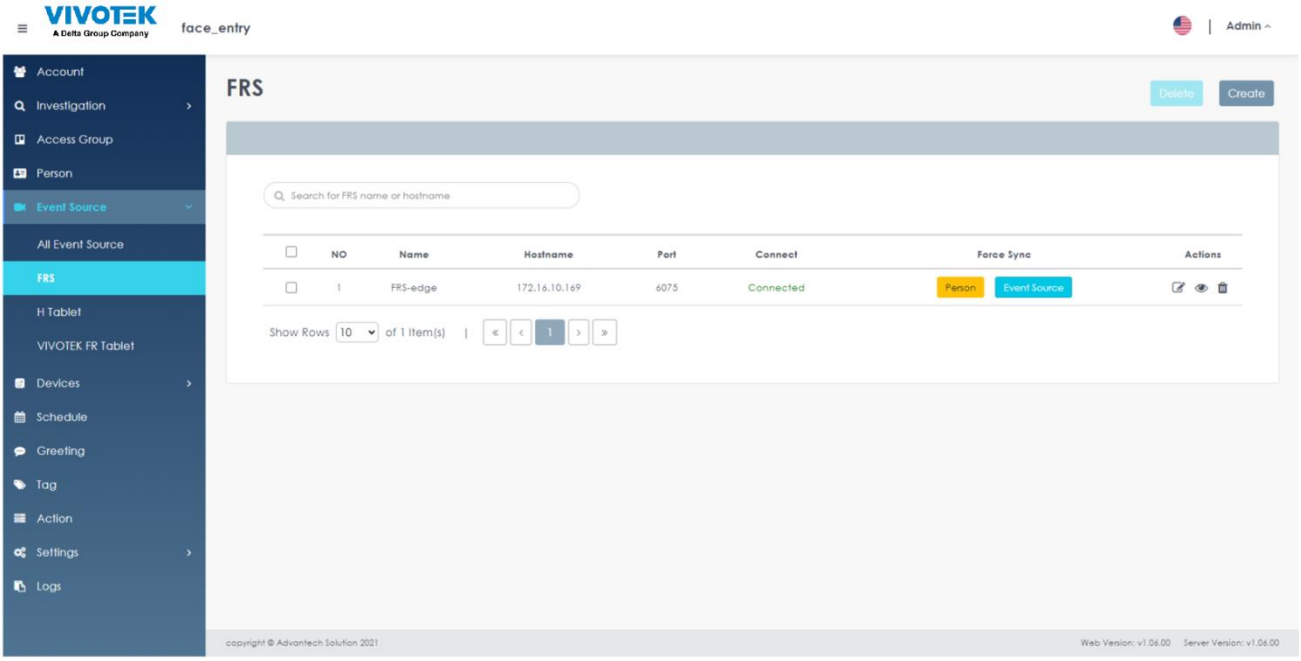


FIGURE 2.43 Face Manager VAST FACE List

4. Use filters to narrow the result range by VAST FACE name or VAST FACE host location
5. Click the "Search" button to display only the information that meets the filter criteria.
6. To view the VAST FACE details, click on the "Details" ⋮ icon and select "View", which will display the full details of the selected data:
    a. VAST FACE Detailed Information
    b. Event Sources List

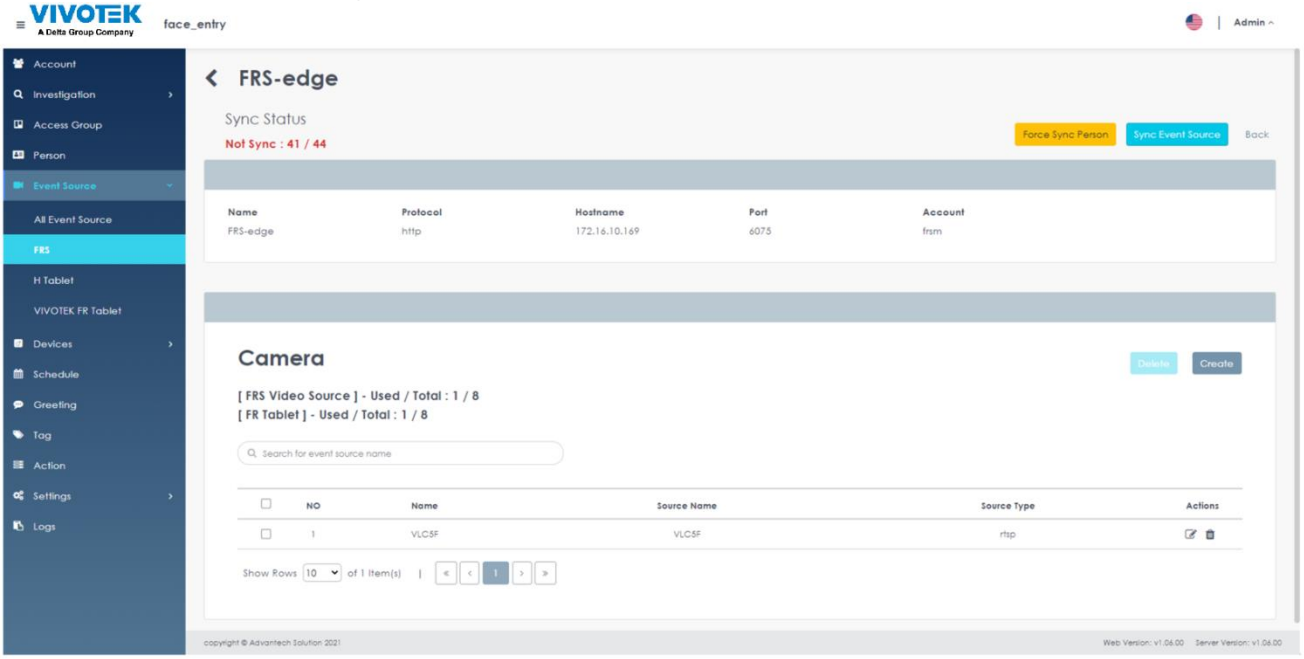


FIGURE 2.44 Face Manager VAST FACE Details

7. To modify the VAST FACE information, please click on the "Edit" button and modify the information according to your needs.

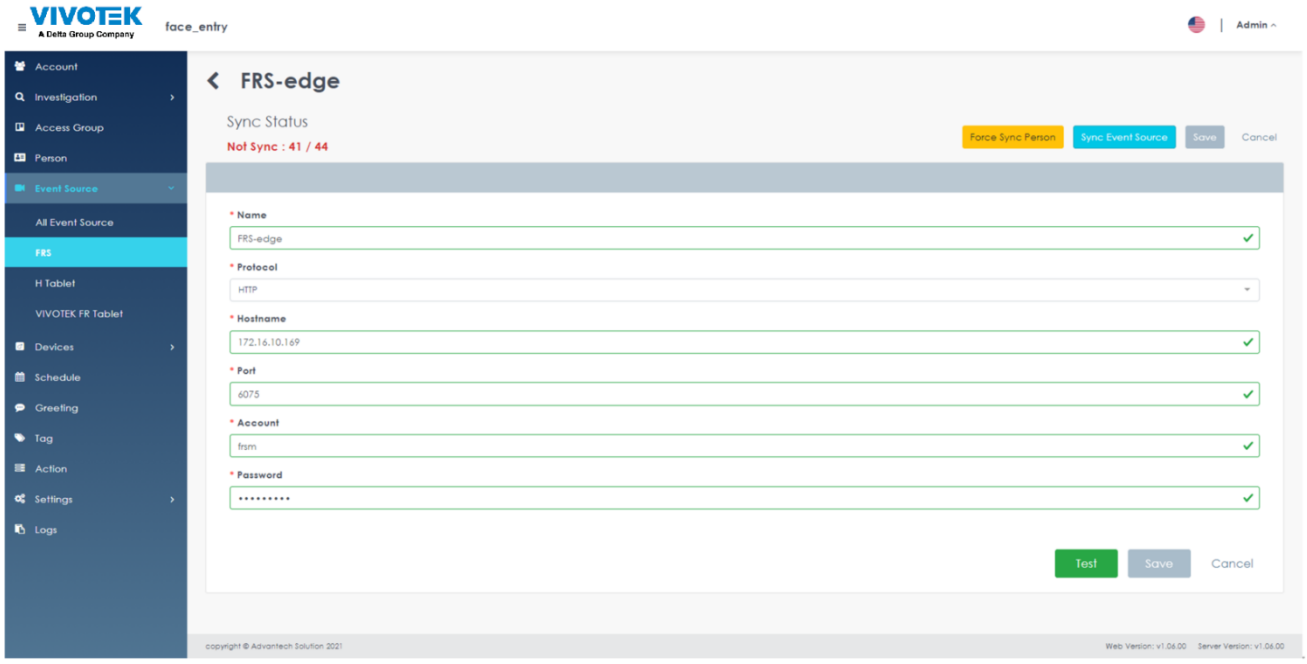


FIGURE 2.1 F Face Manager VAST FACE Edit

8. Click "Save" to apply changes
9. In order to view the details of the image source, click on the "Details" ⋮ icon and select "Modify", which will display the full details of the selected data

10. Modify image source information as required

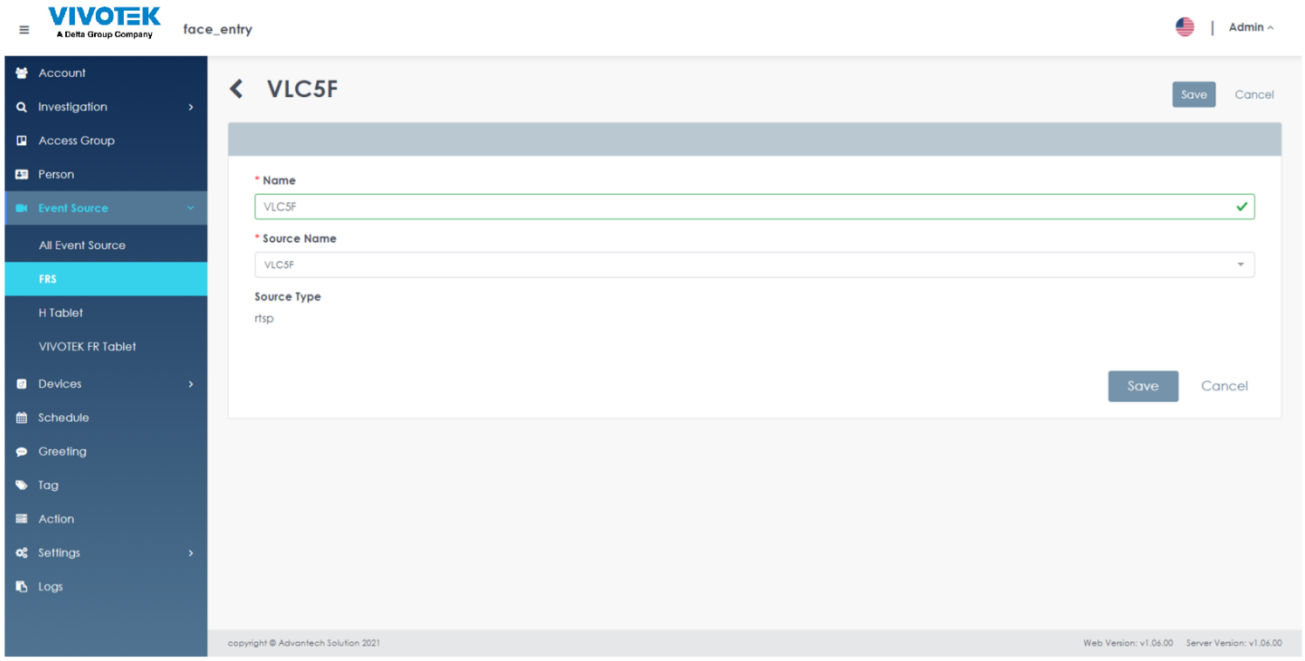


FIGURE 2.45 Face Manager VAST FACE Video Source Edit

11. Click "Save" to apply changes

12. To add image source data, click the "+ Create" button (+ Create)

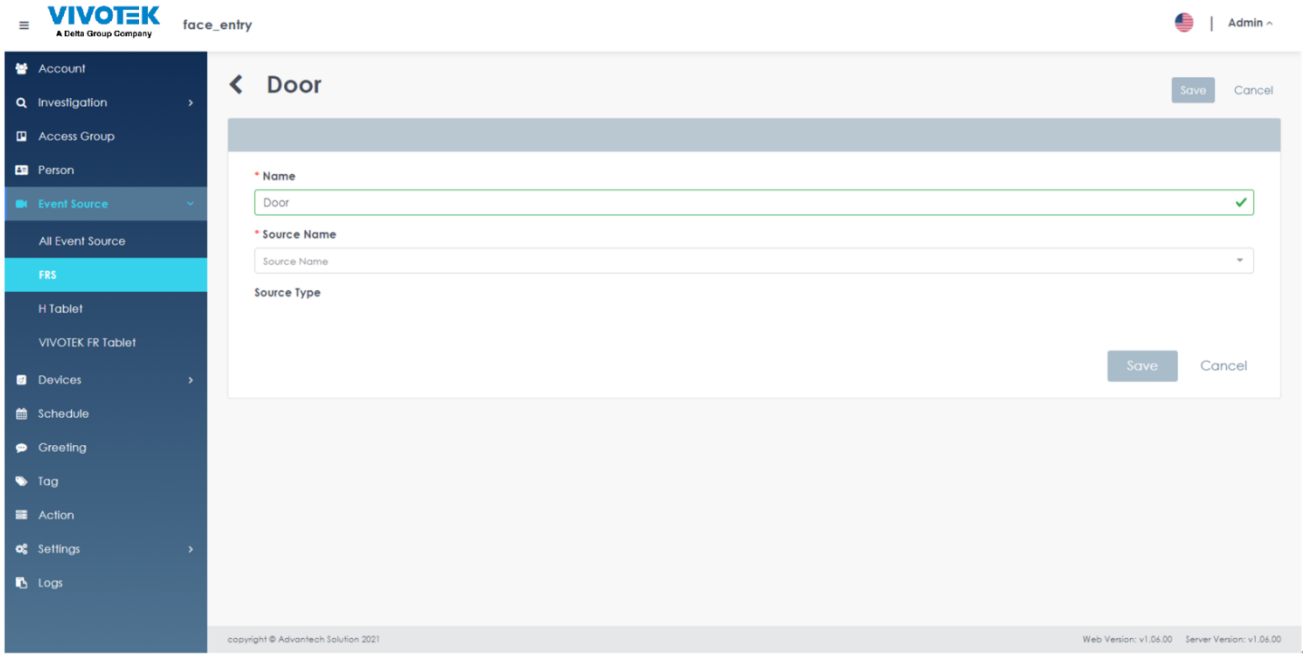


FIGURE 2.46 Face Manager VAST FACE Video Source Create

13. On the "New Source Create" menu, enter data for the new event source:

    a. Event Source Name➡Custom Event Source Name

b. Event Source➡Select from cameras that have been set

c. Event Source Type ➡ (Non-editable) Automatically filled by the system when the event source is selected.

14. Click "Save" to create an event source
15. To delete the event source, click on the "Details" icon ⋮ and select Delete
16. A pop-up window will appear on the screen, prompting the user to confirm the action

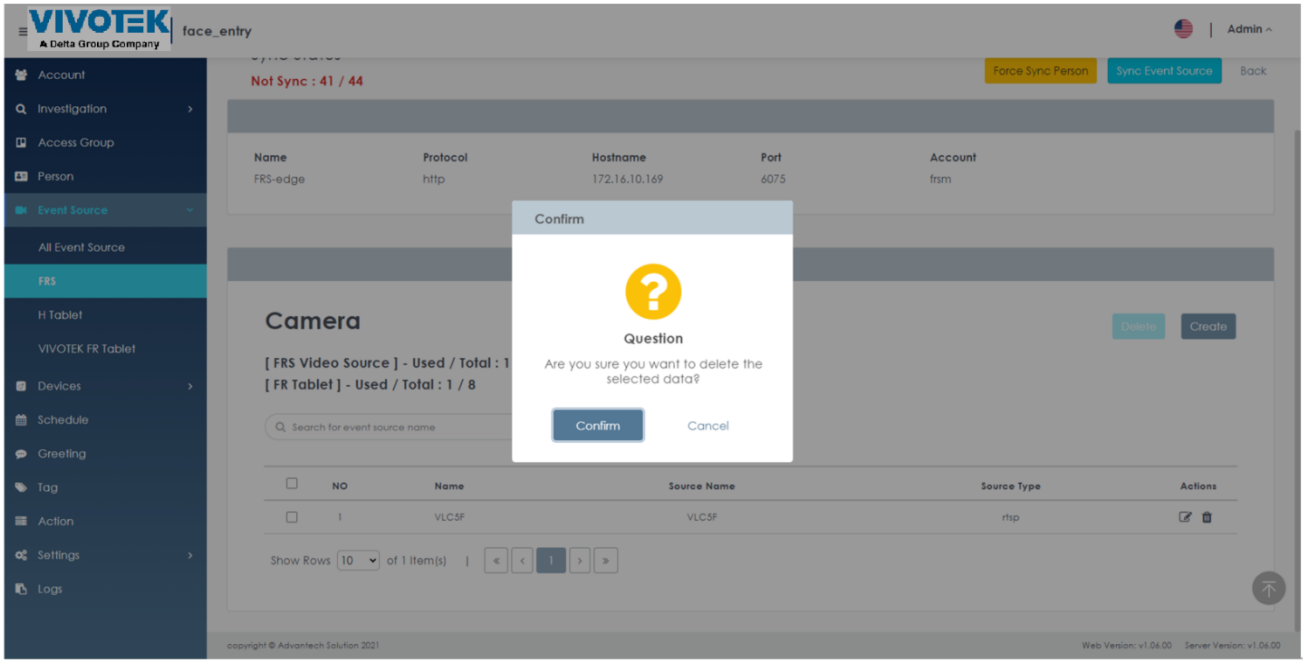


FIGURE 2.47 Face Manager VAST FACE Video Source Delete

17. Click "Confirm" to delete the selected event source data
18. To add VAST FACE data, click the "+ Create" button (+ Create)
19. On the "Create VAST FACE" menu, enter data for the new VAST FACE:

a. VAST FACE Name ➡ Custom VAST FACE Name

b. Protocol ➡ Select protocol for connecting to VAST FACE (HTTP/HTTPS)

c. Hostname ➡ Enter the host location of the VAST FACE to connect to.

d. Port ➡ Enter the port number of the VAST FACE to connect to.

e. Account ➡ Enter the Manager account of the VAST FACE to connect with.

f. Password ➡ Enter the Manager password of the VAST FACE to connect with

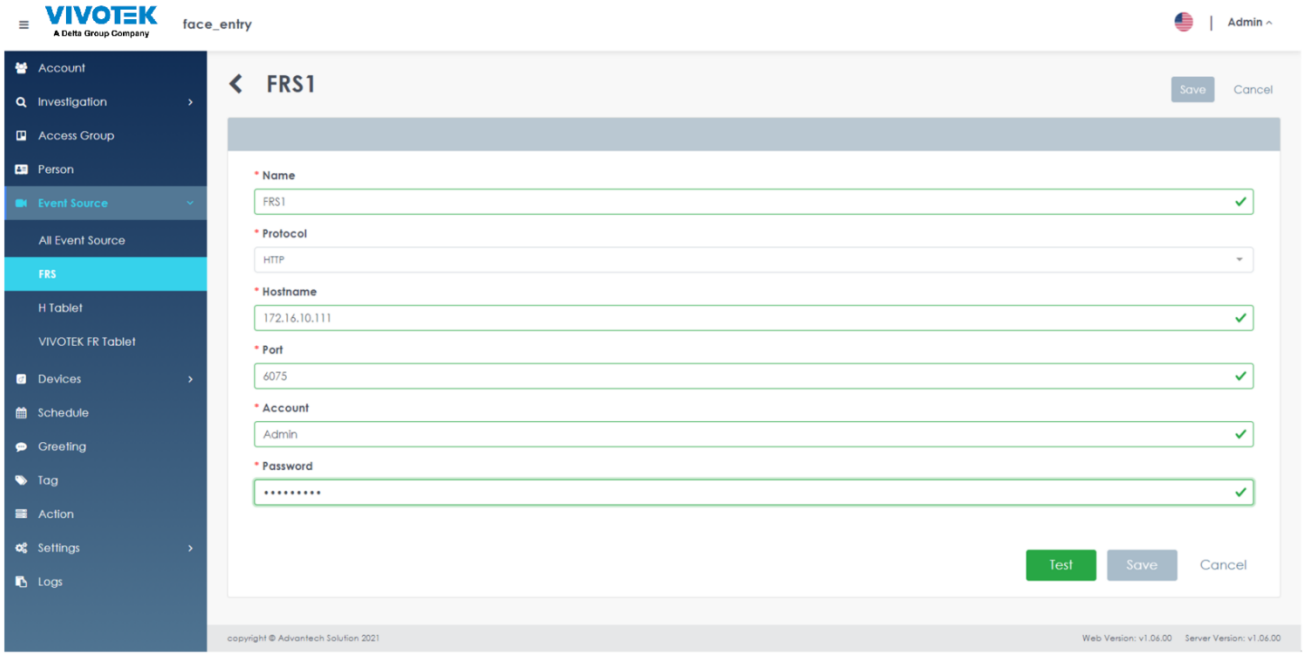


FIGURE 2.48 Face Manager VAST FACE Create

20. Click "Test" to confirm that the VAST FACE connection is working before clicking "Save" to create an VAST FACE connection.
21. To delete the VAST FACE connection, click on the "Details" icon ⋮ and select Delete.
22. A pop-up window will appear on the screen, prompting the user to confirm the action

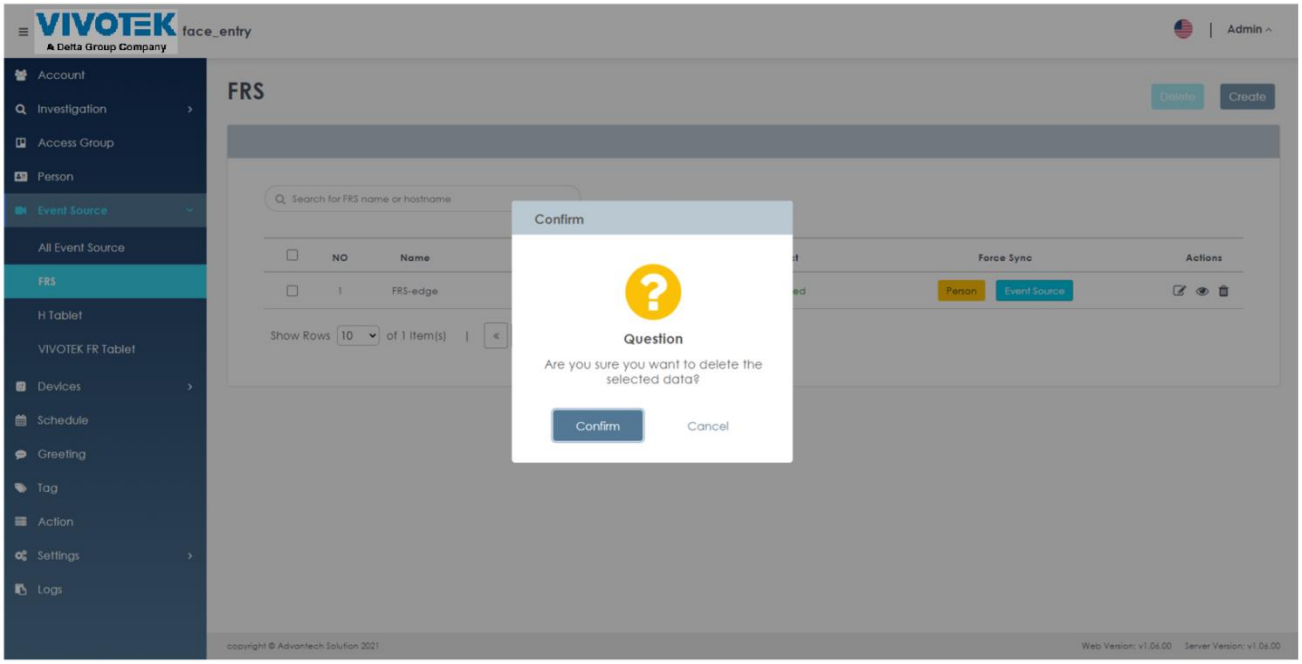


FIGURE 2.49 Face Manager VAST FACE Delete

23. Click "Confirm" to delete the selected VAST FACE connection data

2.8.3 H Tablet Management

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Event Source" menu ➡"H Tablet", which will display a list of all configured H Tablets

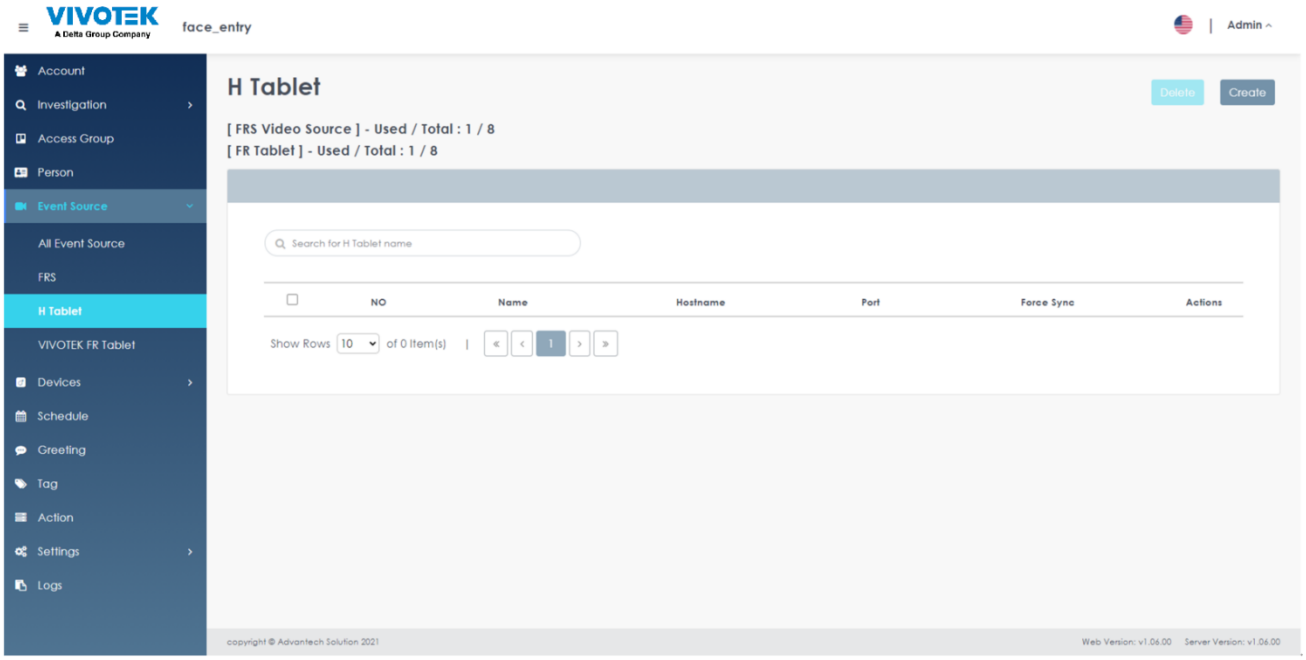


FIGURE 2.50 Face Manager H Tablet List

4. Use filters to narrow down results by tablet name
5. Click the "Search" button to display only the information that meets the filter criteria.
6. In order to view the schedule details, click on the "Details" ⋮ icon and select "Edit", which will display the full details of the selected data
7. Edit any related data as required

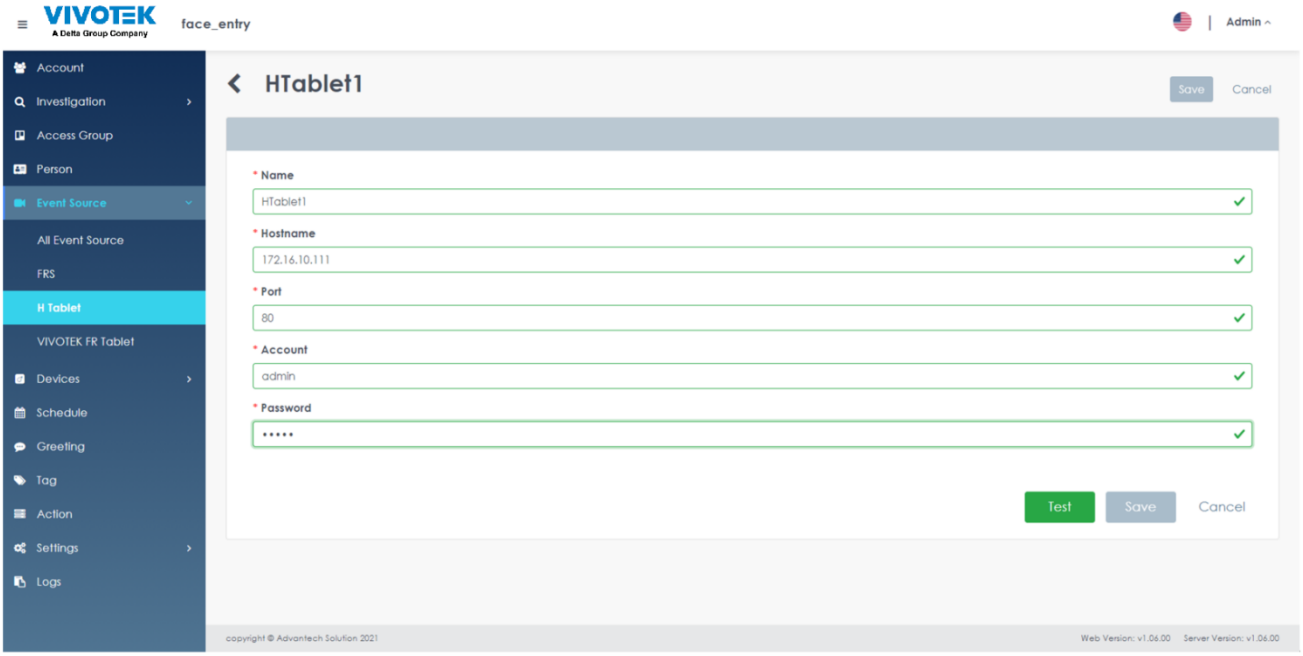


FIGURE 2.51 Face Manager H Tablet Details

8. Click "Save" to apply changes
9. To delete data, click on the "Details" icon ⋮ and select Delete
10. A pop-up window will appear on the screen, prompting the user to confirm the action

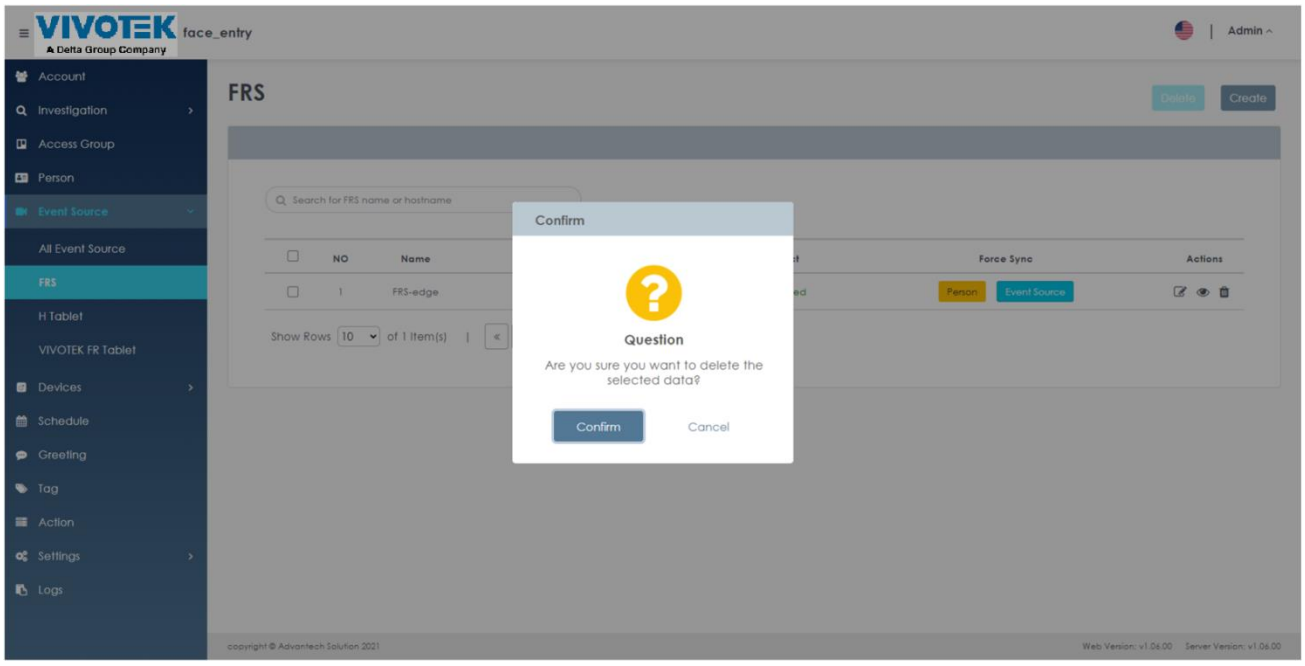


FIGURE 2.52 Face Manager H Tablet Delete

11. Click "Confirm" to delete the selected H Tablet data

12. To add H Tablet data, click the "+ Create" button (+ Create)
13. On the "Create H Tablet" menu, enter data for the new H Tablet:
    a. Event Source Name➡Custom Event Source Name
    b. Hostname ➡ Set host location of the H tablet to connect to
    c. Port ➡ Set port number of the H tablet to connect to
    d. Account ➡ Set the account of the H tablet to connect with
    e. Password ➡ Set the password of the H tablet to connect with

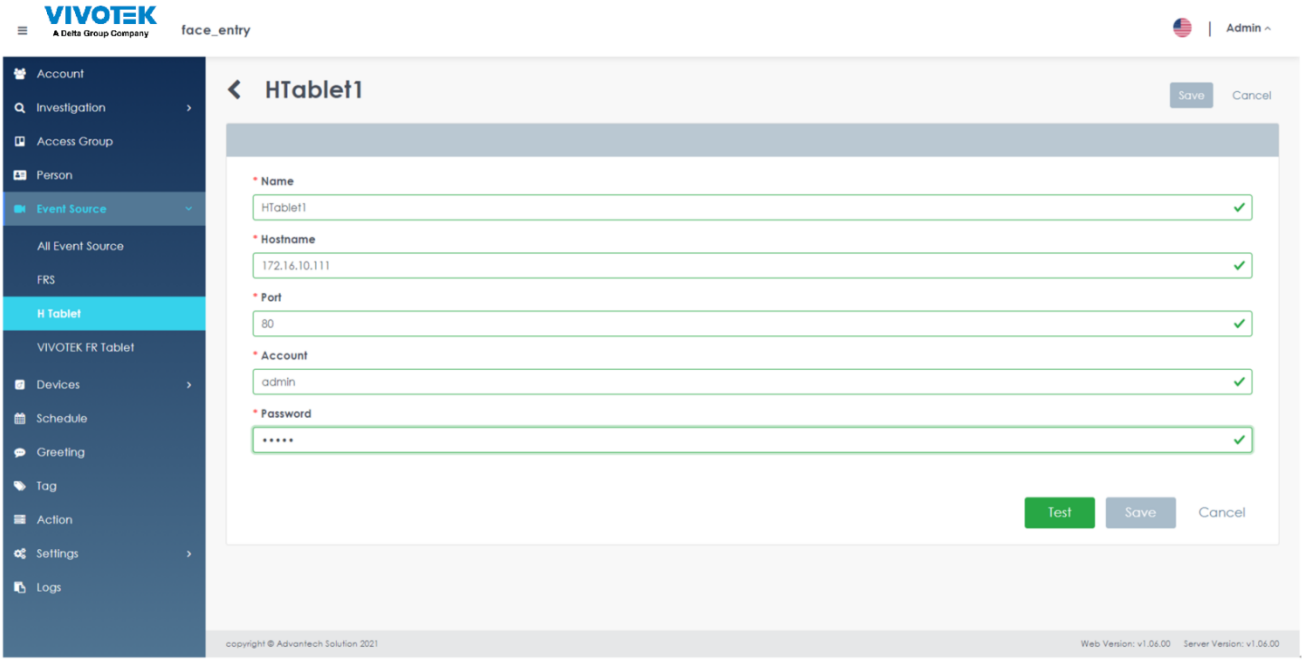


FIGURE 2.53 Face Manager H Tablet Create

14. Click "Save" to create H Tablet

2.8.4 VIVOTEK FR Tablet Management

1. On a Windows PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Event Source" menu ➡ "VIVOTEK FR Tablet", which will display a list of all configured VIVOTEK FR Tablets

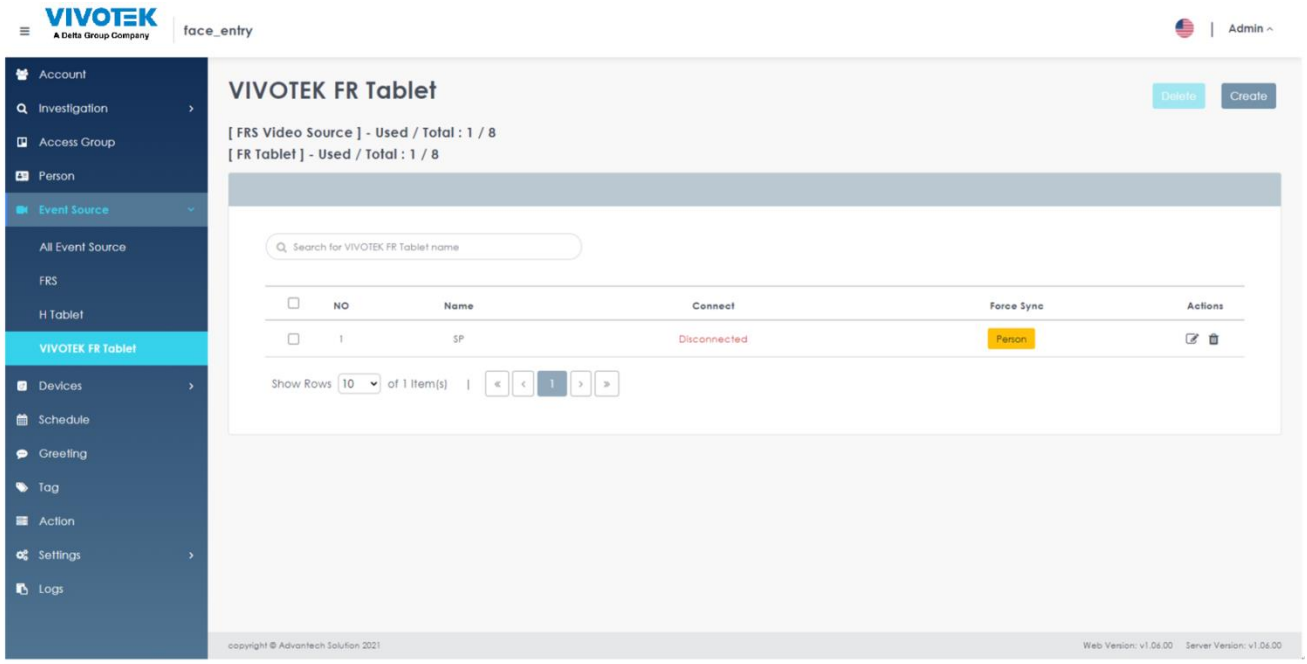


FIGURE 2.54 Face Manager VIVOTEK FR Tablet List

4. Use filters to narrow down results by tablet name
5. Click the "Search" button to display only the information that meets the filter criteria.
6. In order to view the schedule details, click on the "Details" ⋮ icon and select "Edit", which will display the full details of the selected data
7. Edit any related data as required

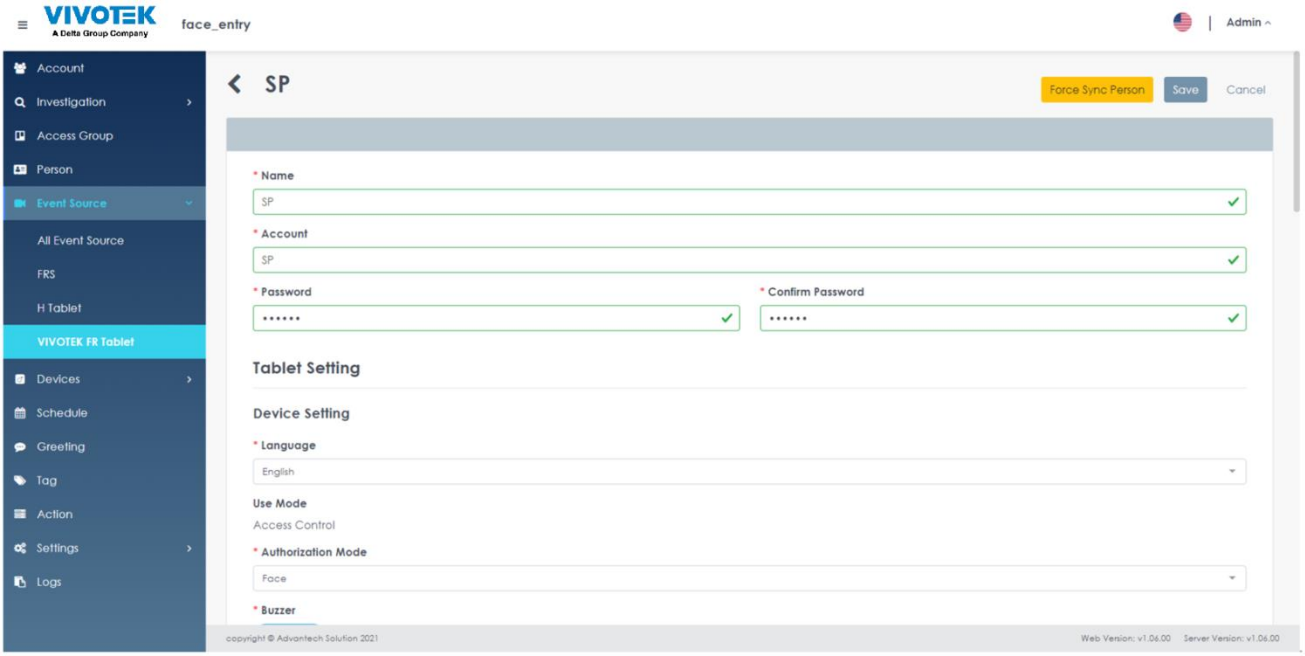


FIGURE 2.55 Face Manager VIVOTEK FR Tablet Details

8. Click "Save" to apply changes
9. To delete data, click on the "Details" icon ⋮ and select Delete
10. A pop-up window will appear on the screen, prompting the user to confirm the action

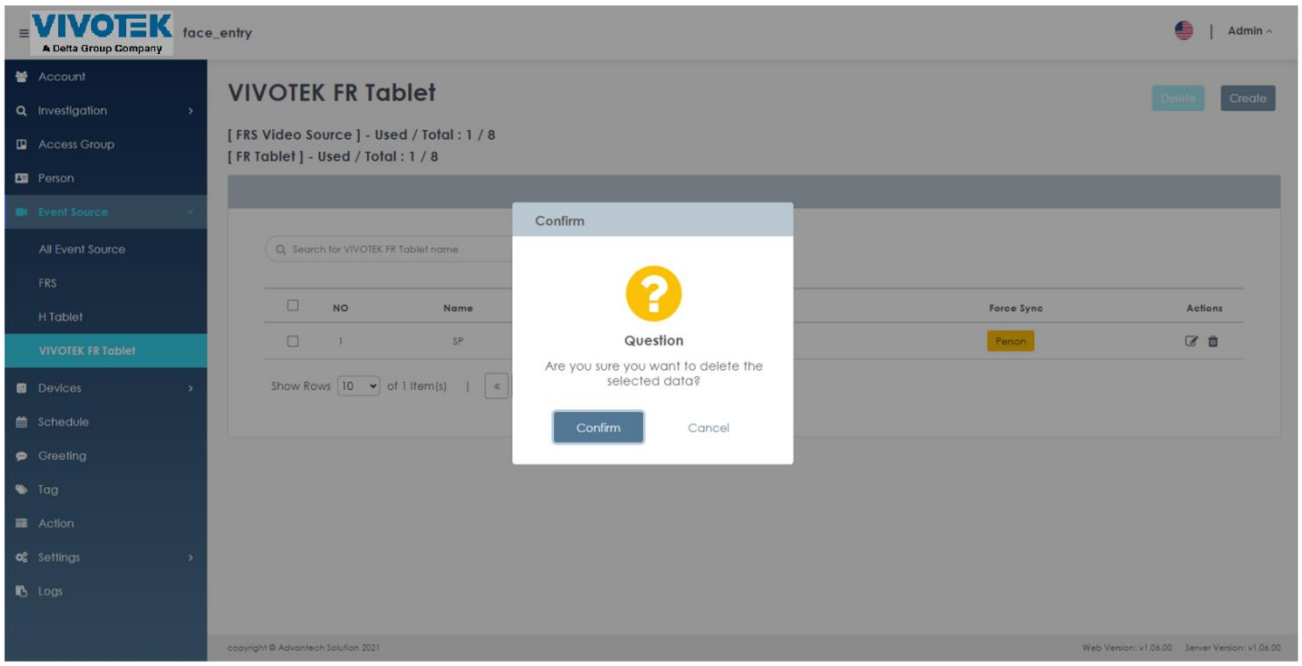


FIGURE 2.56 Face Manager VIVOTEK FR Tablet Delete

11. Click "Confirm" to delete the selected VIVOTEK FR Tablet data

12. To add VIVOTEK FR Tablet data, click the "+ Create" button ()

13. On the "Setup VIVOTEK FR Tablet" menu, enter the new VIVOTEK FR Tablet information.

    a. VIVOTEK FR Tablet Name ➡ VIVOTEK FR Tablet Name

    b. Account ➡ account to connect to the VIVOTEK FR Tablet.

    c. Password ➡ password to connect to the VIVOTEK FR Tablet

    d. Reconfirm Password ➡ verify password for the VIVOTEK FR Tablet flat panel connection.

    e. Language ➡ Set language for the tablet display

    f. Use mode ➡ (not editable) Fixed to access control mode

    g. Authentication mode ➡ Face, card and QR code can be selected as authentication method

    h. Buzzer ➡After turning on the detection of the corresponding abnormalities will trigger an alarm, close the local no buzzer alarm

    i. Auto Restart ➡ If Auto Restart is turned on, you can set the restart time

    j. Door opening method ➡ Trigger action after successful recognition can be selected

    k. GPIO-A output point ➡ (optional) Device that can be triggered after recognition failure

    l. GPIO-B input port ➡ (optional) can trigger the abnormal event report of the tablet

    m. GPIO-C input port ➡ (optional) can trigger the abnormal event report of the tablet

    n. Wiegand entrance ➡ (optional) by swiping the card to open the door, if this setting is required, card verification is required in the verification mode

    o. Liveness Detection ➡ Turn on to avoid face recognition in photos or videos

    p. Liveness detection threshold value ➡ (range: 0-1) Accuracy of live detection can be set

    q. Face Recognition Threshold (Range: 0-1) ➡ The minimum face recognition reliability (also known as the match rate) between the captured image and the registered face in the database. A higher value (from 0.0 to 1.0) indicates that the event needs to be more similar to a standard sample image and the system marks the event as a positive face recognition

    r. Recognition distance ➡ Set the recognition detection distance

    s. Auto light compensation ➡ When the device detects that the brightness is below a certain value and the infrared distance sensor detects someone, the recognition page will automatically switch to the fill light page to achieve face fill light through the background, thus realizing normal face recognition. If there is no one, the page will be switched to the normal recognition page again. Intelligent switching of the fill light background can realize the fill light in dark conditions, and the non-continuous maintenance of the fill light background can prolong the life of the screen.

    t. Welcome Message displayed ➡ self-defined message when tablet is on standby mode

    u. Authentication Success display message ➡ self-defined message upon successful recognition

    v. Authentication Failure display message ➡ self-defined message upon recognition failed

    w. Standby mode ➡ If on, the device will automatically enter standby mode when no one passes for a period of time, the standby mode will turn off the camera and other functions, which can reduce

power consumption and extend the life of the device. When someone is detected approaching or clicking the screen, the device will automatically enter the recognition page and run normally.

x. Trigger facial recognition distance ➡ Set facial recognition distance

y. Display Staff Work ID number ➡ Select whether or not to display the employee's work number.

z. Display Staff functional title ➡ Select whether to show staff title

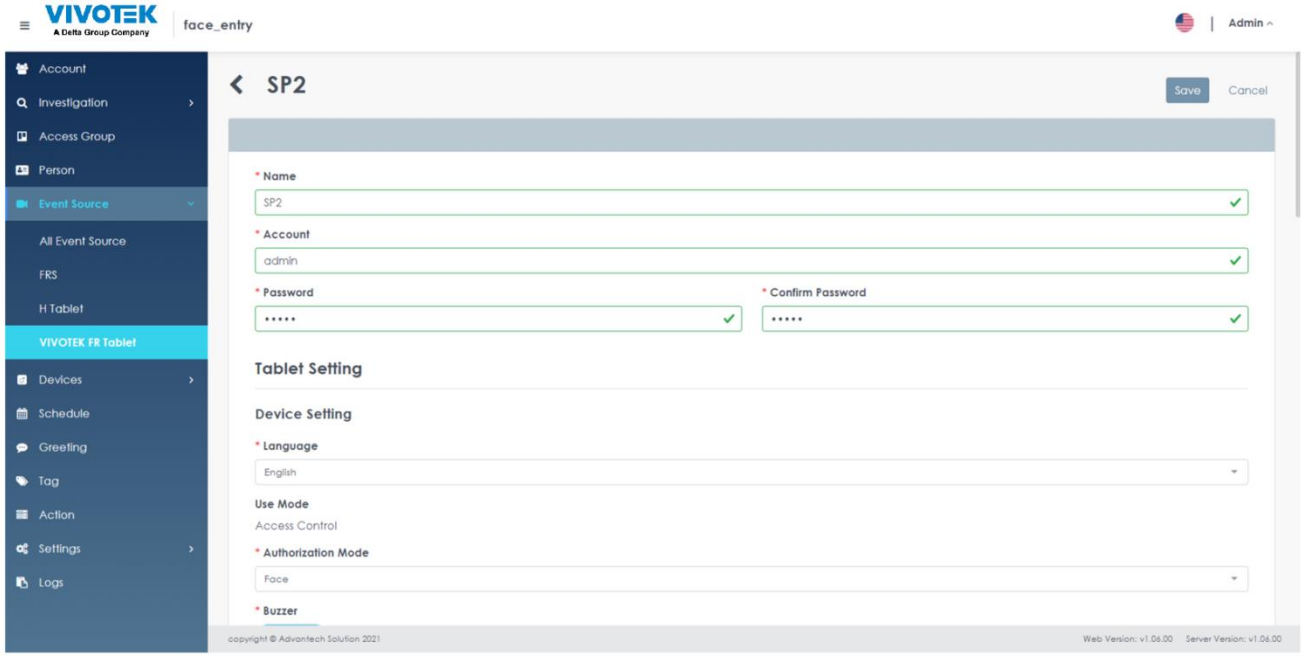


FIGURE 2.57 Face Manager VIVOTEK FR Tablet Create

14. Click "Save" to setup VIVOTEK FR Tablet

2.9 Device Management

2.9.1 I/O Box

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login Face Manager server with Administrator credentials

3. Navigate to "I/O Box" in the "Device" menu, which will display all the setup I/O Box information

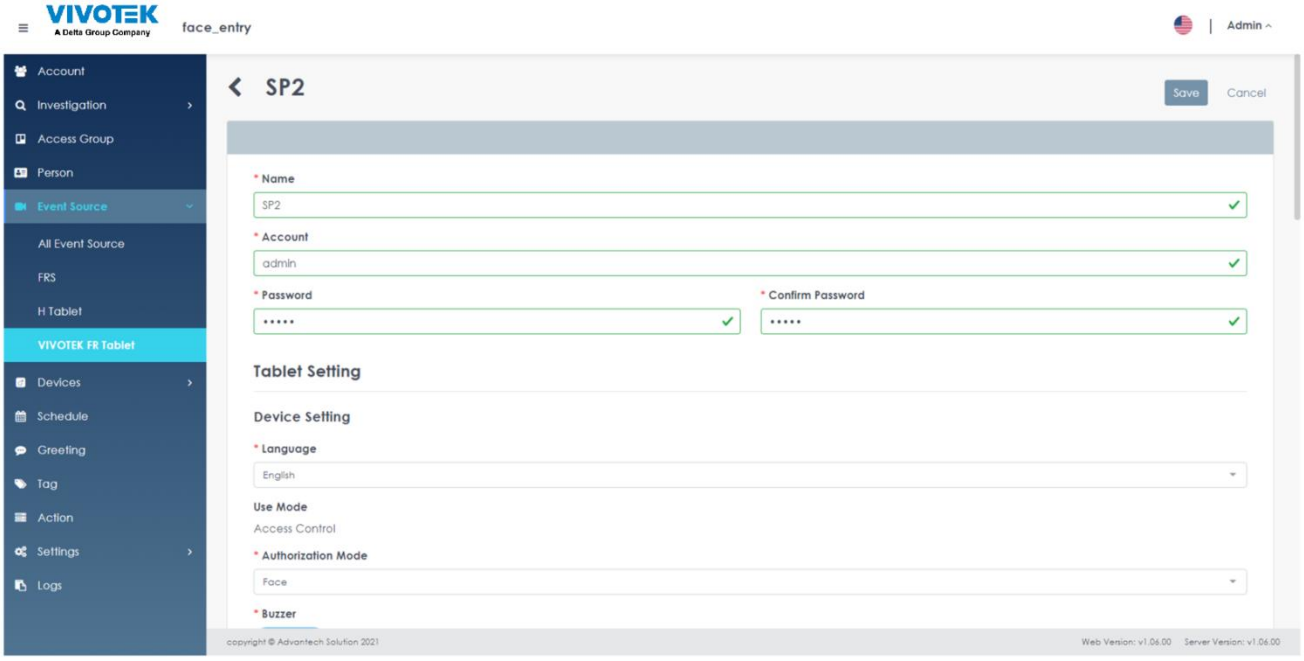


FIGURE 2.58 Face Manager Device List

4. To view the details of the I/O Box, click on the "Details" icon and select "Modify", which will display the full details of the selected I/O Box

5. Modify any required changes

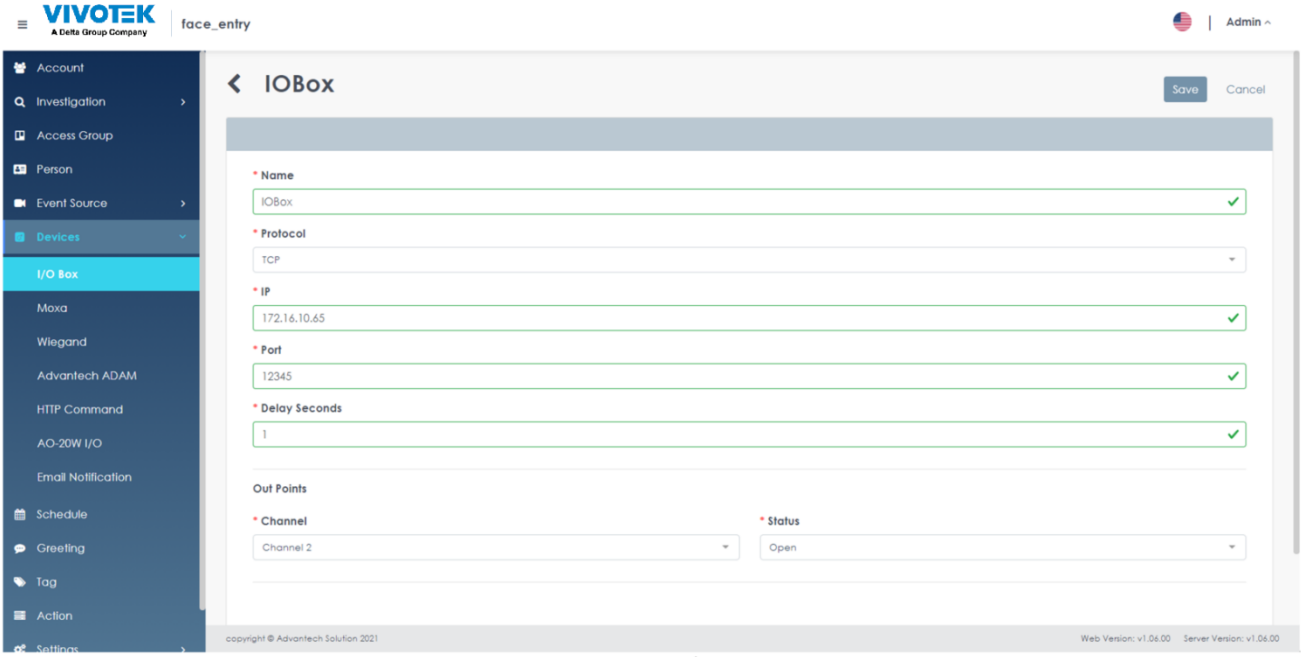


FIGURE 2.59 Device - I/O Box details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon (⋮) and select Delete (Delete)
8. A pop-up window will appear on the screen, prompting the user to confirm the action

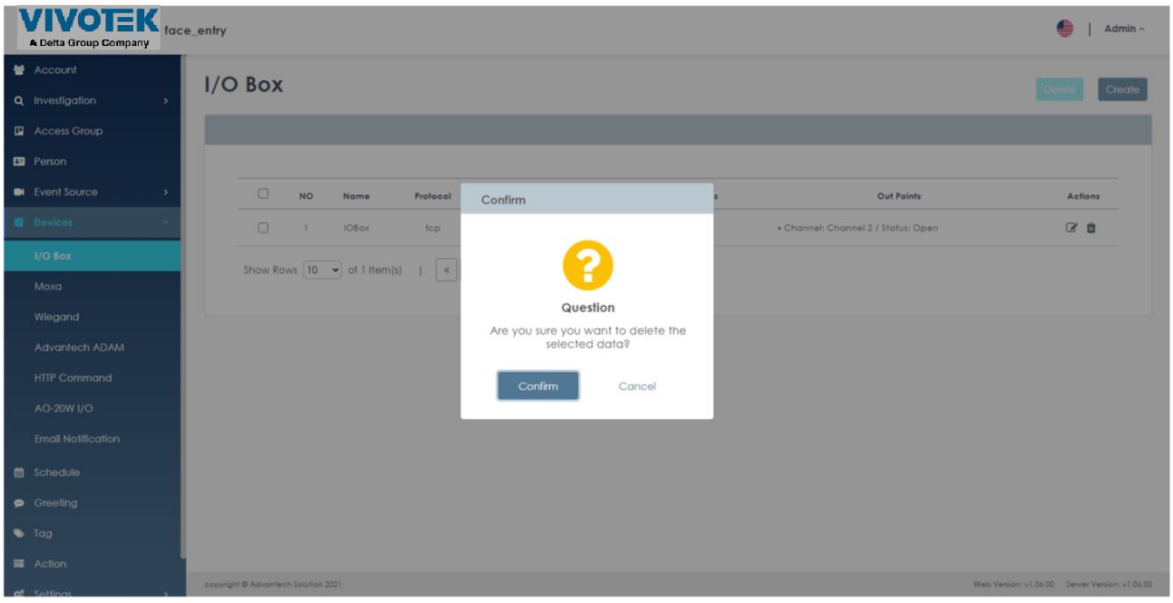


FIGURE 2.60 Device delete I/O Box

9. Click "Confirm" to delete the selected I/O Box data
10. To add I/O Box data, click the "+ Create" button (+ Create).

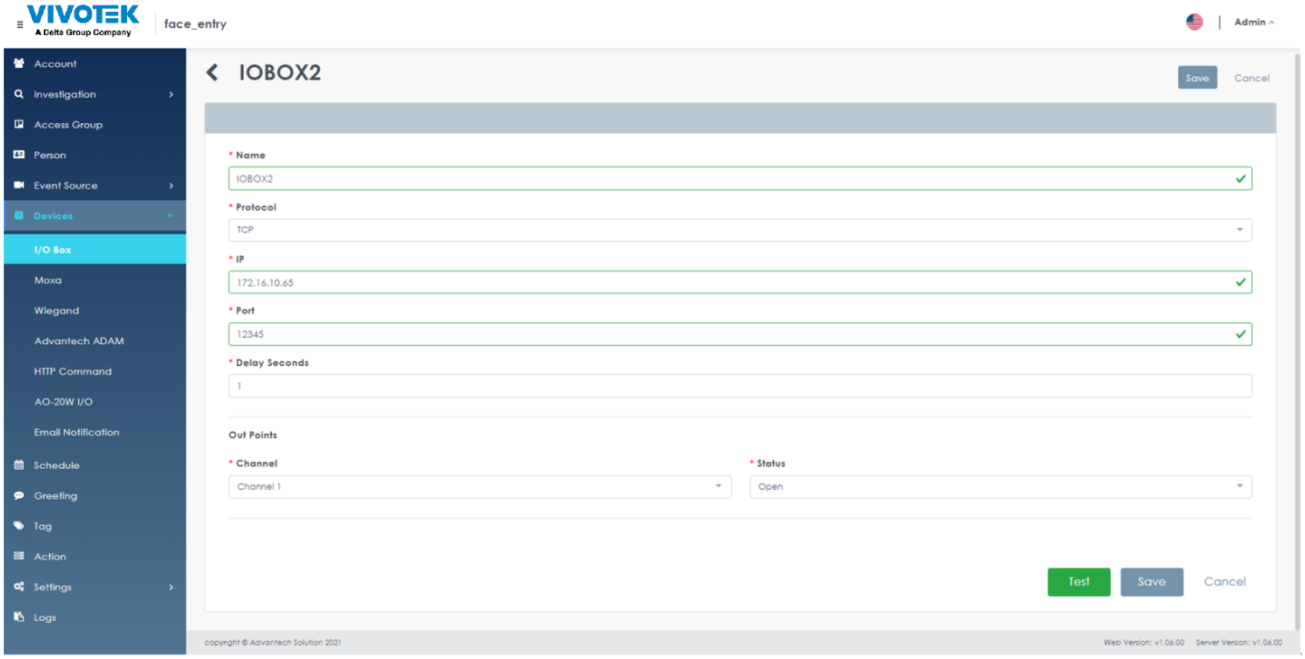


FIGURE 2.61 DEVICE - CREATE I/O BOX

11. On the "Create I/O Box" menu, enter the new I/O Box related information.
    a. Name ➡ self-defined I/O Box Name
    b. Protocol ➡ Select protocol (TCP / UDP) for connecting to the I/O Box
    c. IP setting ➡ setup IP address of the I/O Box
    d. Port Setting ➡ setup port number to connect to this I/O Box
    e. Delay seconds Setting ➡ setup required time delay after each action triggered by the I/O Box, after the delay time, the I/O Box will return to the original state.

Remark

- The original status of I/O Box depends on the trigger state, if the trigger state is "On", the original state is "Off", and vice versa if the trigger state is "Off", the original state is "On".

    f. Trigger Location Set the DO output (Channel 1 / Channel 2) and trigger status (on/off) of ➡the I/O Box.

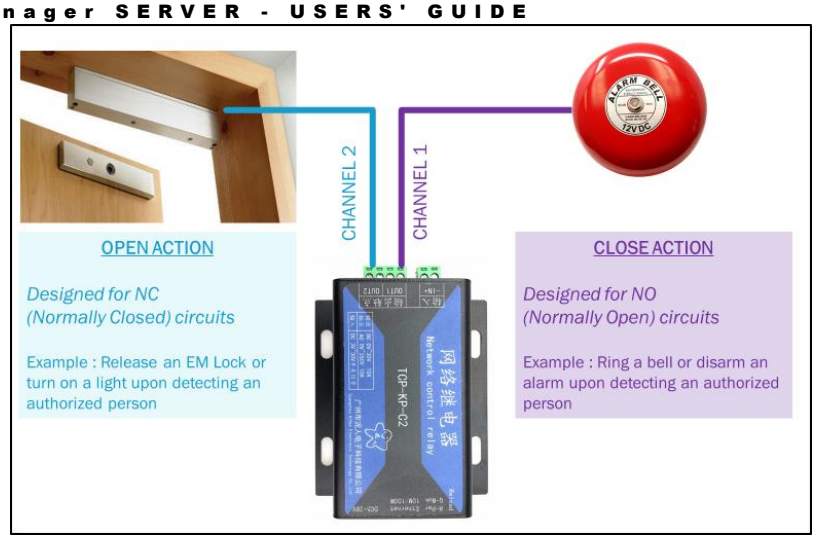


FIGURE 2.62 Channel and status explanation.

12. Click "Test" to test if the IP and port can be properly connected to the I/O Box, if the test fails, the device data cannot be saved
13. Click "Save" to create I/O Box data

2.9.2 Moxa

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login to Face Manager server with Administrator credentials

3. Navigate to "➡Moxa" in the "Devices" menu, which will show all the created Moxa I/O data

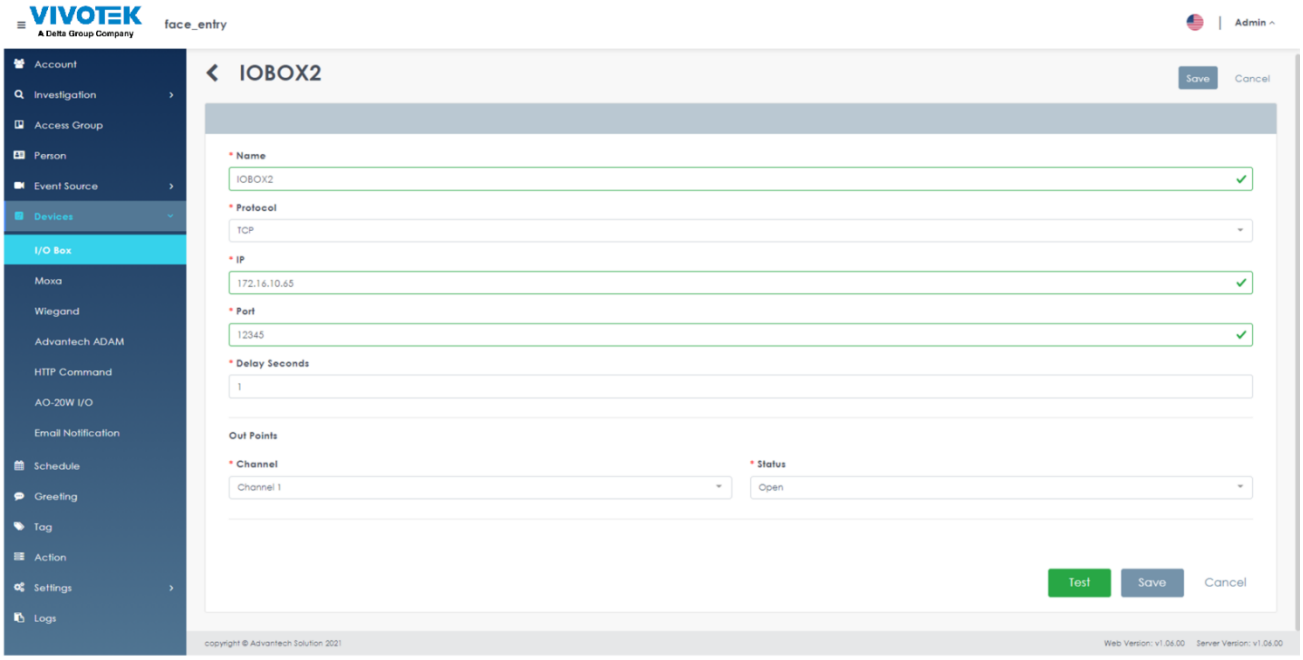


FIGURE 2.63 Device - Moxa I/O list

4. To view the details of the Moxa I/O, click on the "Details" ⋮ icon and select "Modify", which will display the full details of the selected Moxa I/O

5. Modify any required changes

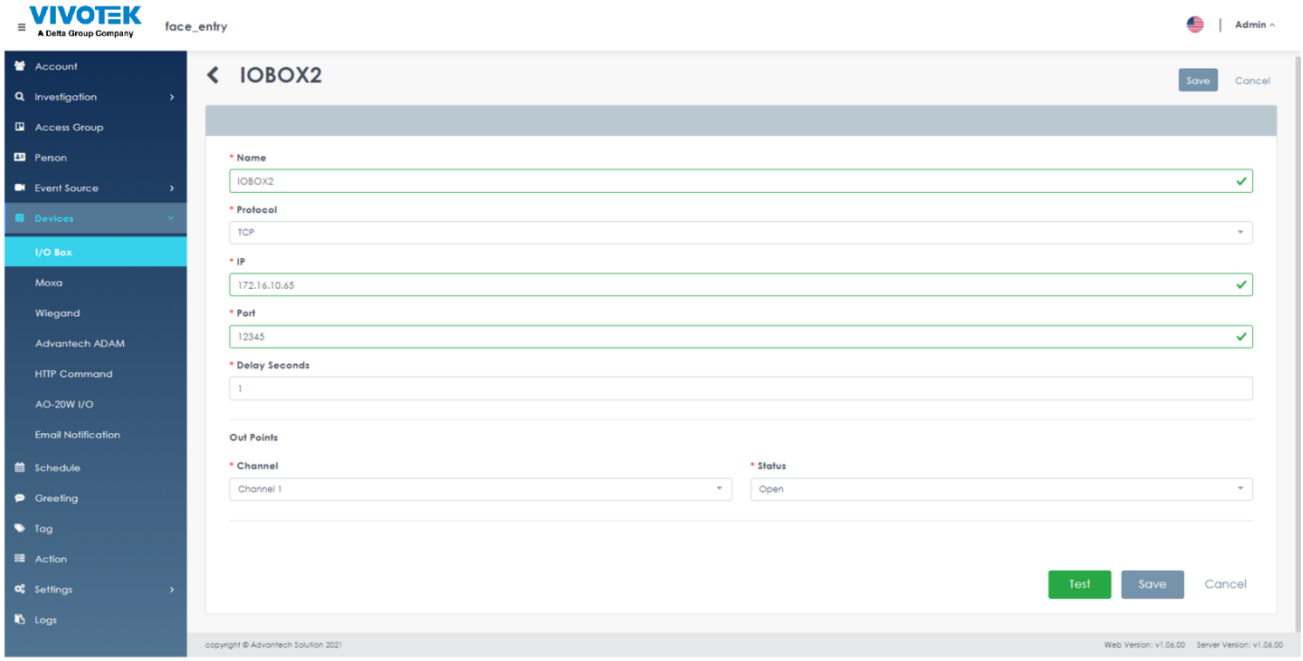


FIGURE 2.64 Device - Moxa details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon (⋮) and select Delete (Delete)
8. A pop-up window will appear on the screen, prompting the user to confirm the action

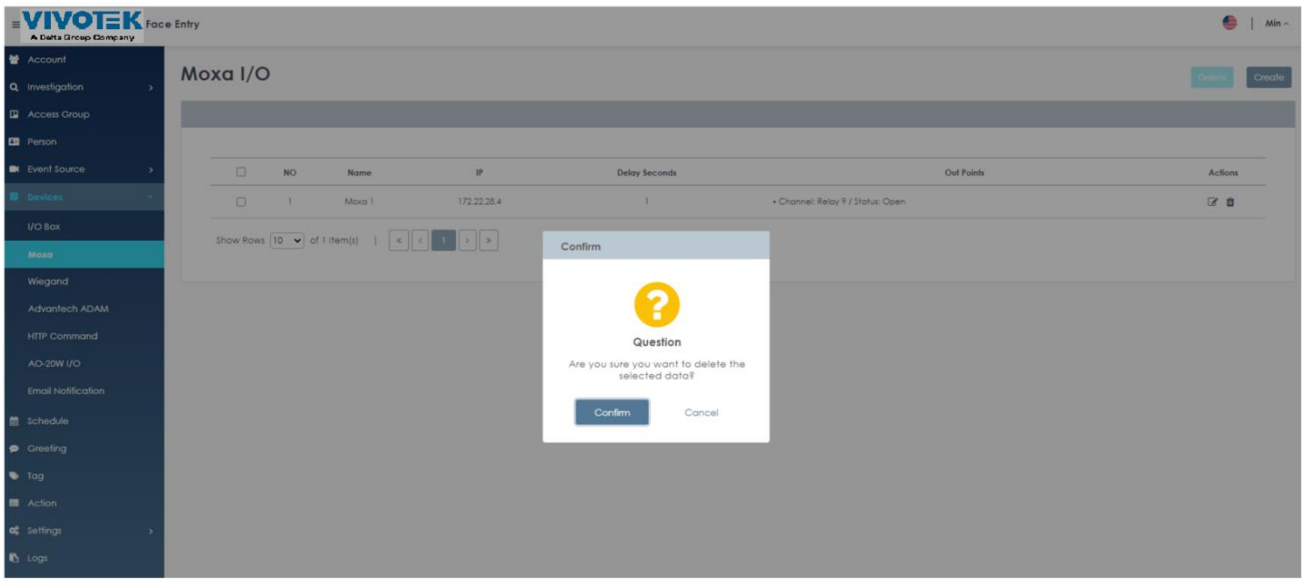


FIGURE 2.65 Device delete Moxa

9. Click "Confirm" to delete the selected Moxa I/O data
10. To add Moxa I/O data, click the "+ Create" button (+ Create).

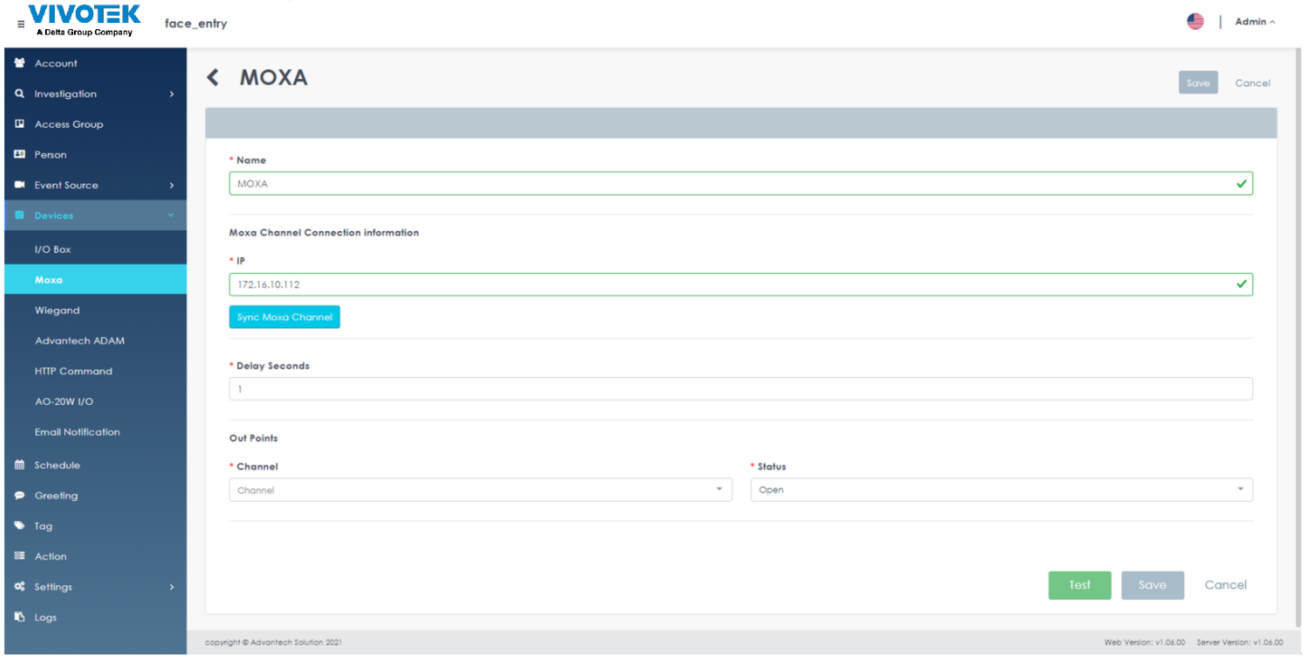


FIGURE 2.66 Device - create Moxa

11. On the "Create Moxa" menu, enter the new Moxa I/O data message.
    a. Name ➡ self-defined Moxa I/O Name
    b. Delay seconds ➡ Set the delay time which the Moxa I/O will remain after each action trigger state change, after which the Moxa I/O will return to its original state

Remark

- The original state of Moxa I/O depends on the trigger state, if the trigger state is "On", the original state is "Off", and vice versa if the trigger state is "Off", the original state is "On".

    c. IP settings and the➡ address of the connection to the Moxa I/O
    d. Synchronize Moxa links to get the➡Moxa I/O with several DO outputs
    e. Trigger position Set which DO output (Channel 1 / Channel 2) and trigger status (on/off) for ➡the Moxa I/O.

12. Click "Test" to test if the IP can connect to the Moxa I/O correctly, if the test fails, the device data cannot be saved
13. Click "Save" to create Moxa I/O data

2.9.3 Wiegand

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login to Face Manager server with Administrator credentials

3. Navigate to "➡Wiegand" in the "Devices" menu, which will show all the created Wiegand data

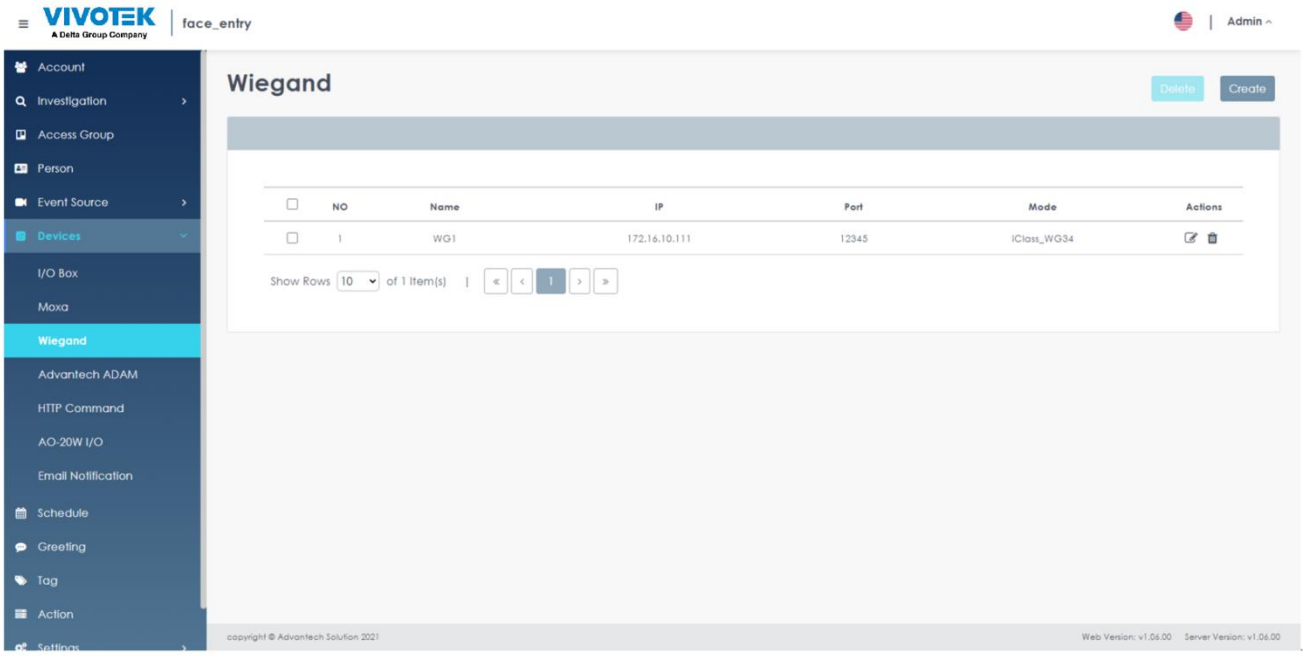


FIGURE 2.67 Device - Wiegand list

4. To view the Wiegand details, click on the "Details" ⋮ icon and select "Modify" to display the full details of the selected Wiegand

5. Modify any required changes

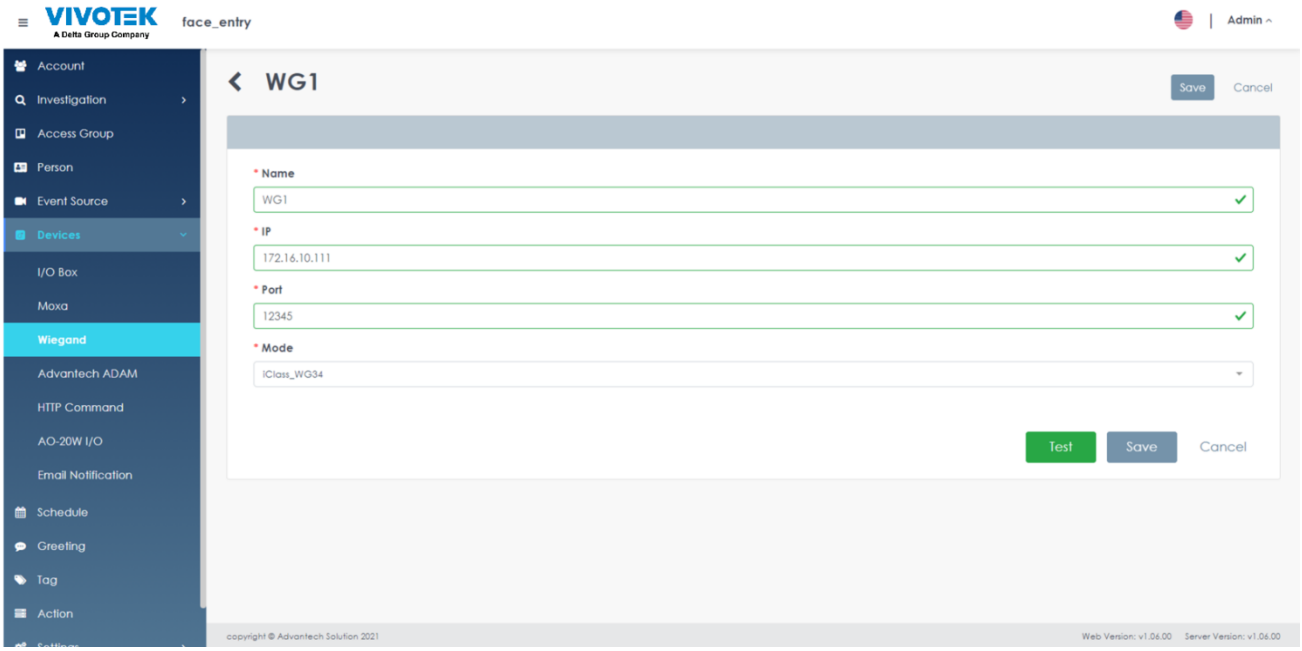


FIGURE 2.68 Device - Wiegand details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon ( ) and select Delete (Delete)
8. A pop-up window will appear on the screen, prompting the user to confirm the action

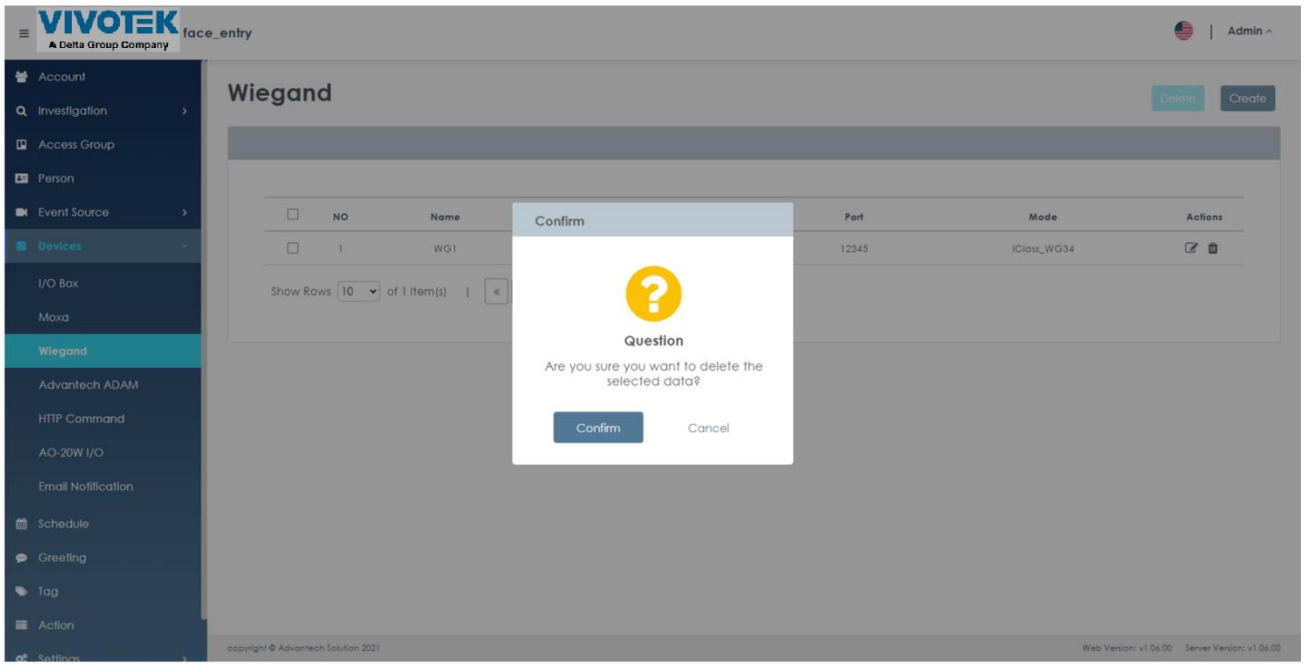


FIGURE 2.69 Device delete Wieand

9. Click "Confirm" to delete the selected Wiegand data
10. To add Wiegand data, click the "+ Create" button (+ Create).

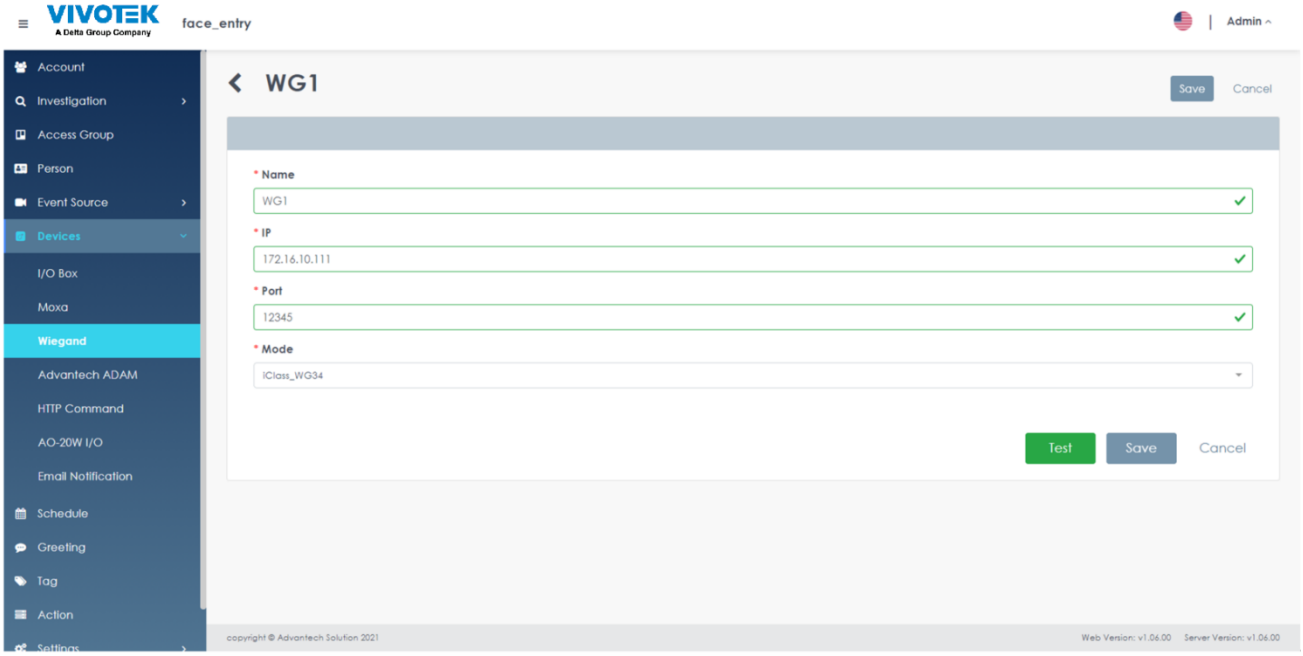


FIGURE 2.70 Device - create Wiegand

11. On the "Create Wiegand" menu, enter the new Wiegand data message.
    a. Name Custom➡Wiegand Name
    b. IP address to set➡connection with the Wiegand
    c. Port Set➡port number to connect to this Wiegand
    d. Mode➡ Corresponding to the Card technology (iClass or Mifare) and Wiegand bit (26 or 34) formats that the converter will output
12. Click "Test" to test if the IP and port can connect to the Wiegand correctly, if the test fails, the device data cannot be saved.
13. Click "Save" to create Wiegand data

2.9.4 Advantech ADAM

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login to Face Manager server with Administrator credentials

3. Navigate to the "Devices" menu "➡Advantech ADAM", which will display all the created Advantech ADAM data

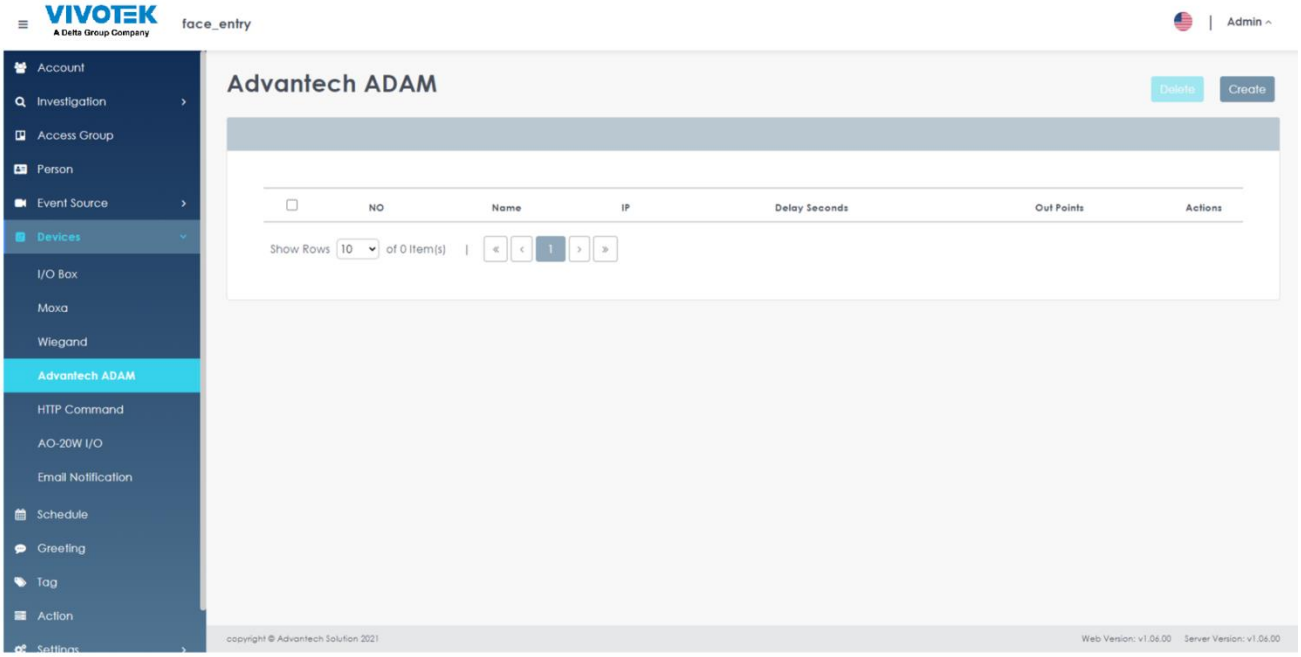


FIGURE 2.71 DEVICE - Advantech ADAM list

4. To view the details of the Advantech ADAM, click on the "Details" ⋮ icon and select "Modify", which will display the full details of the selected Advantech ADAM

5. Modify any required changes

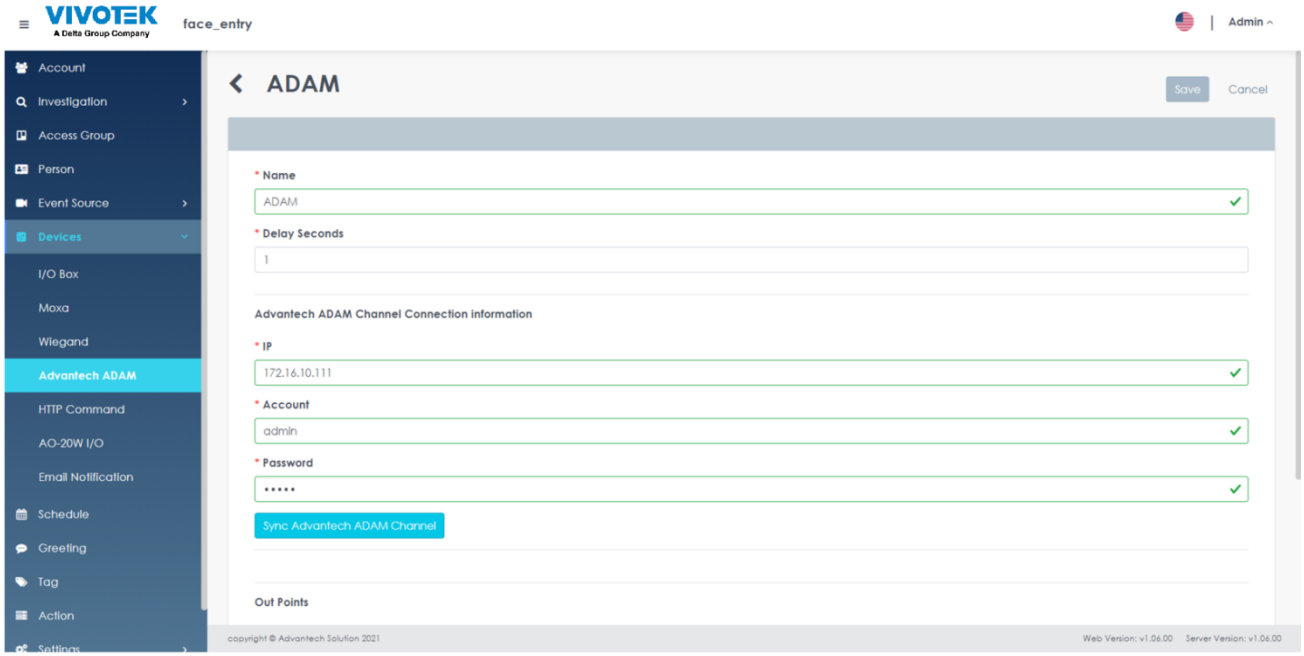


FIGURE 2.72 Device - Advantech ADAM details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon (⋮) and select Delete (Delete)
8. A pop-up window will appear on the screen, prompting the user to confirm the action

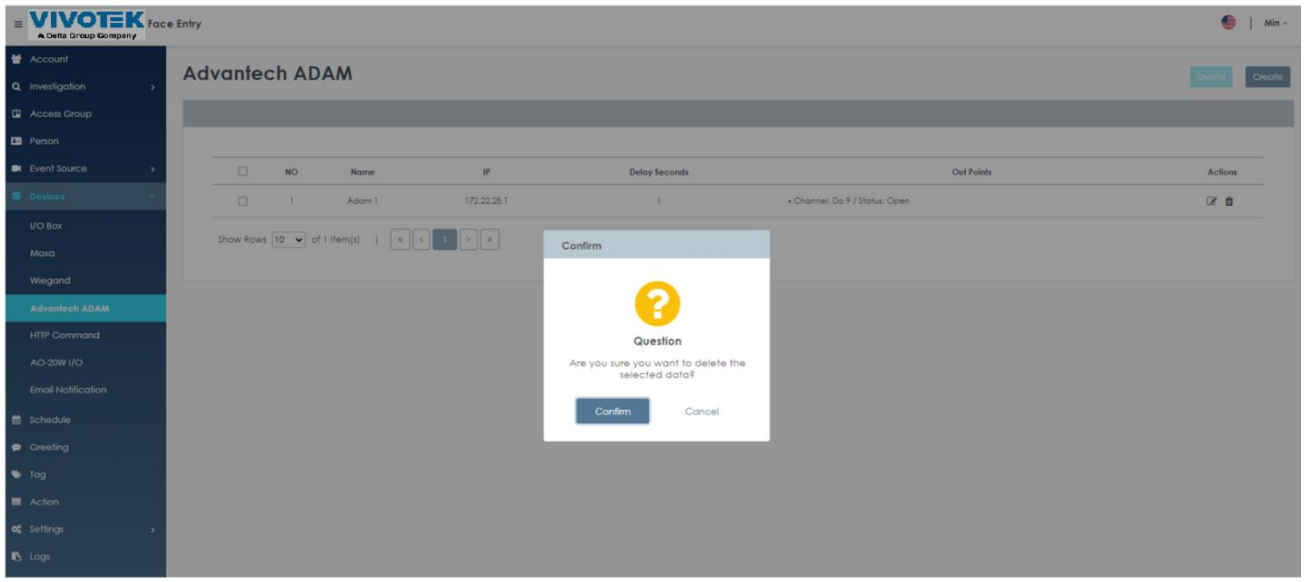


FIGURE 2.73 Device delete Advantech ADAM

9. Click "Confirm" to delete the selected Advantech ADAM data
10. To add Advantech ADAM data, click the "+ Create" button (+ Create).

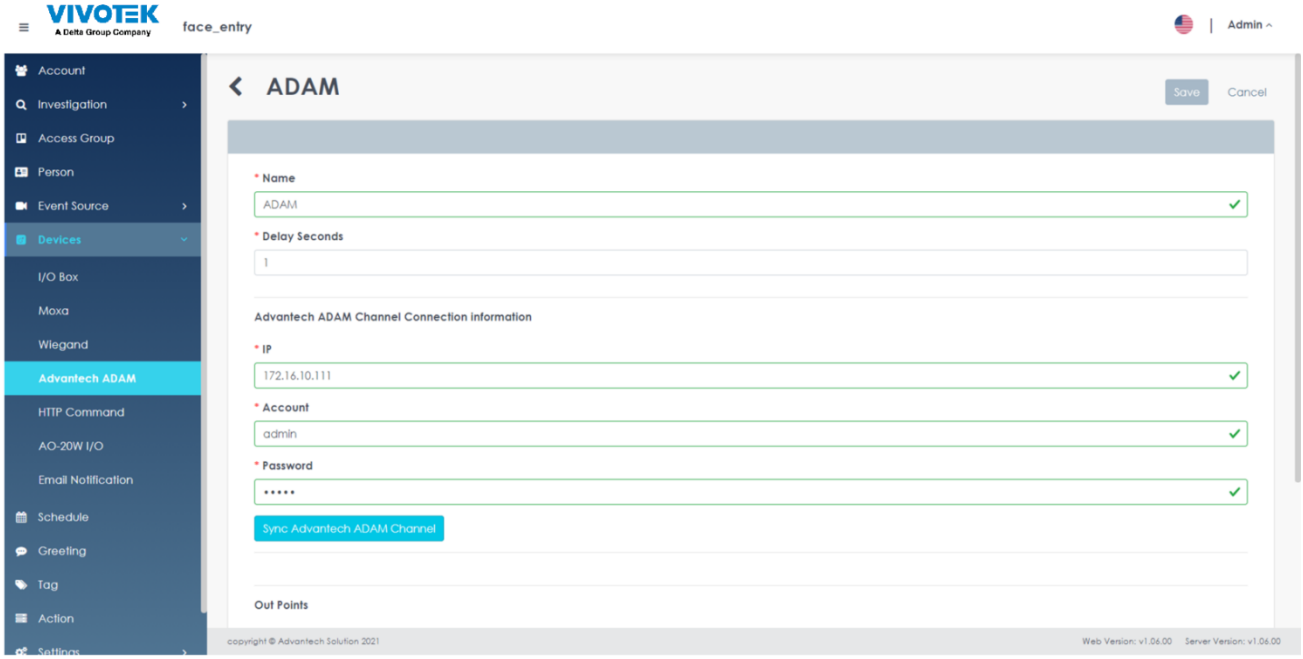


FIGURE 2.74 Device - create Advantech ADAM

11. On the "Create Advantech ADAM" menu, enter the new Advantech ADAM data message:.
    a. Name ➡Customized Advantech ADAM Name
    b. Delay Seconds Set the time after each action trigger state change of ➡the Advantech ADAM, after the delay time, the Advantech ADAM will return to the original state.

Remark

- The original state of Advantech ADAM depends on the trigger state, if the trigger state is "On", the original state is "Off", and vice versa if the trigger state is "Off", the original state is "On".

    c. IP settings and the➡ connection address of this Advantech ADAM
    d. Account Create an account for ➡Advantech ADAM to connect to the server
    e. Password Create the password to connect ➡Advantech ADAM to the server
    f. Synchronize the Advantech ADAM link to obtain the➡Advantech ADAM has several DO outputs
    g. Trigger Location Set which DO output (Channel 1 / Channel 2) and trigger status (on/off) of ➡the Advantech ADAM.
12. Click "Test" to test if the IP can connect to the Advantech ADAM correctly, if the test fails, the device data cannot be saved
13. Click "Save" to create Advantech ADAM data

2.9.5 HTTP Command

If there is a need to notify external systems when people belonging to a face group are detected, Face Manager provides an effective and simple integration method that allows notifications to be sent to third-party systems using

HTTP RESTful APIs. To make it more flexible, notification methods can be defined and the content of notification messages can be customized to meet the requirements.

Remark

- Since the configuration steps are very similar for the same device type, this section will only cover one device model of each type. The only differences are the port number and whether the device requires an account and password. In general, when available, the external device must be set to TCP Server or UDP Server Mode.
- At the time of writing this user manual, only JSON format is supported
- Although users can define their own field names in HTTP template messages, the field values are limited to a list of predefined variables. These variables can be invoked by using double-acronym brackets and variable names. Similarly, variables can be used in the body message or as part of the target URL. For example.

The recognized person's name is Jay, and the emplyoeed number # is 24768547

Host: http://172.16.10.43/alarm?personName={{ personName }}

body:

```
{
    "personEmployeeId":"{{ personEmployeeId }}"
}
```

After triggering the action, the variables on the host and body will be replaced by

Host: http://172.16.10.43/alarm?personName=Jay

body:

```
{
    "personEmployeeId": "24768547"
}
```

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page
2. Login to Face Manager server with Administrator credentials
3. Navigate to the "Device" menu "➡HTTP Command", which will show all the created HTTP Command data

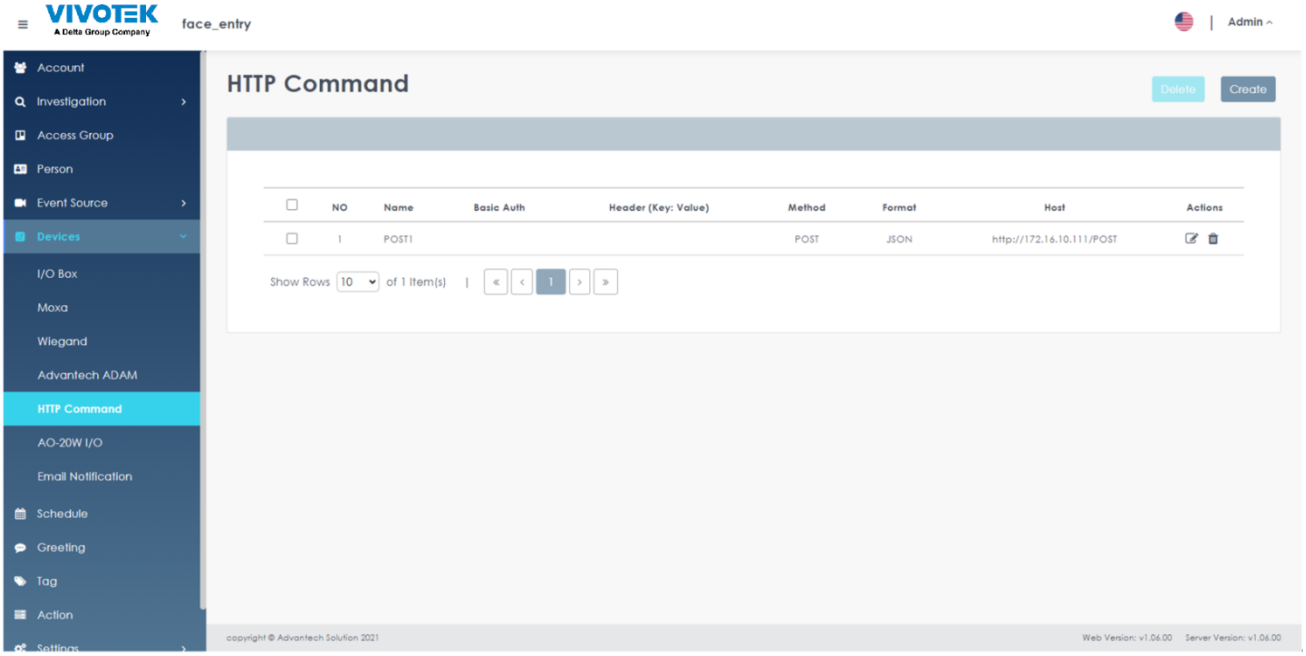


FIGURE 2.75 Device - HTTP Command list

4. To view the details of the HTTP Command, click on the "Details" ⋮ icon and select "Modify", which will display the full details of the selected HTTP Command
5. Modify any required changes

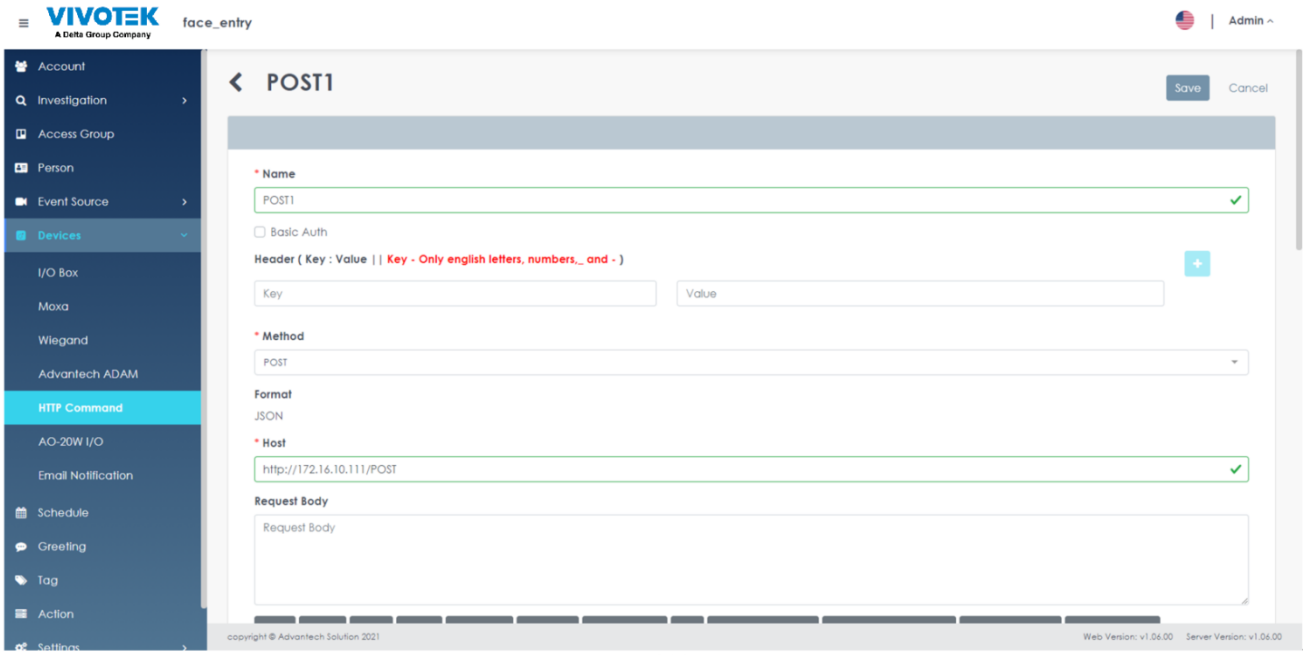


FIGURE 2.76 Device - HTTP Command details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon (⋮ and select Delete (🗑 Delete

8. A pop-up window will appear on the screen, prompting the user to confirm the action

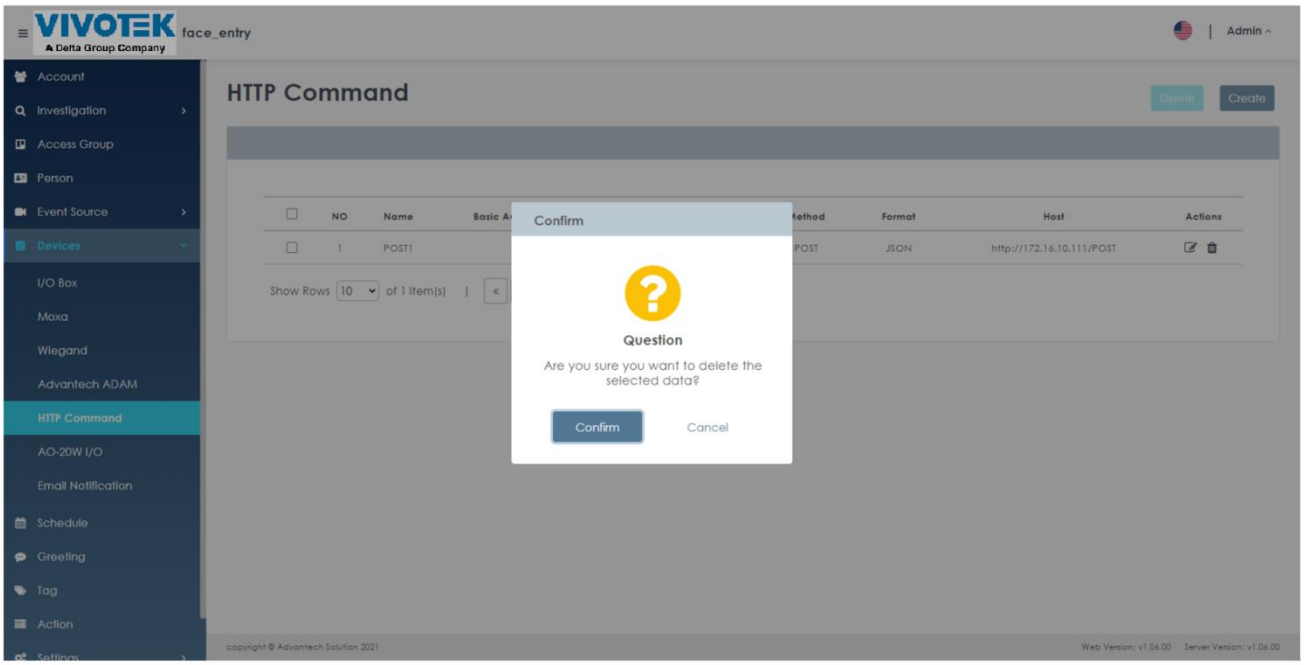


FIGURE 2.77 Device delete HTTP Command

9. Click "Confirm" to delete the selected HTTP Command data

10. To add HTTP Command data, click the "+ Create" button (+ Create).

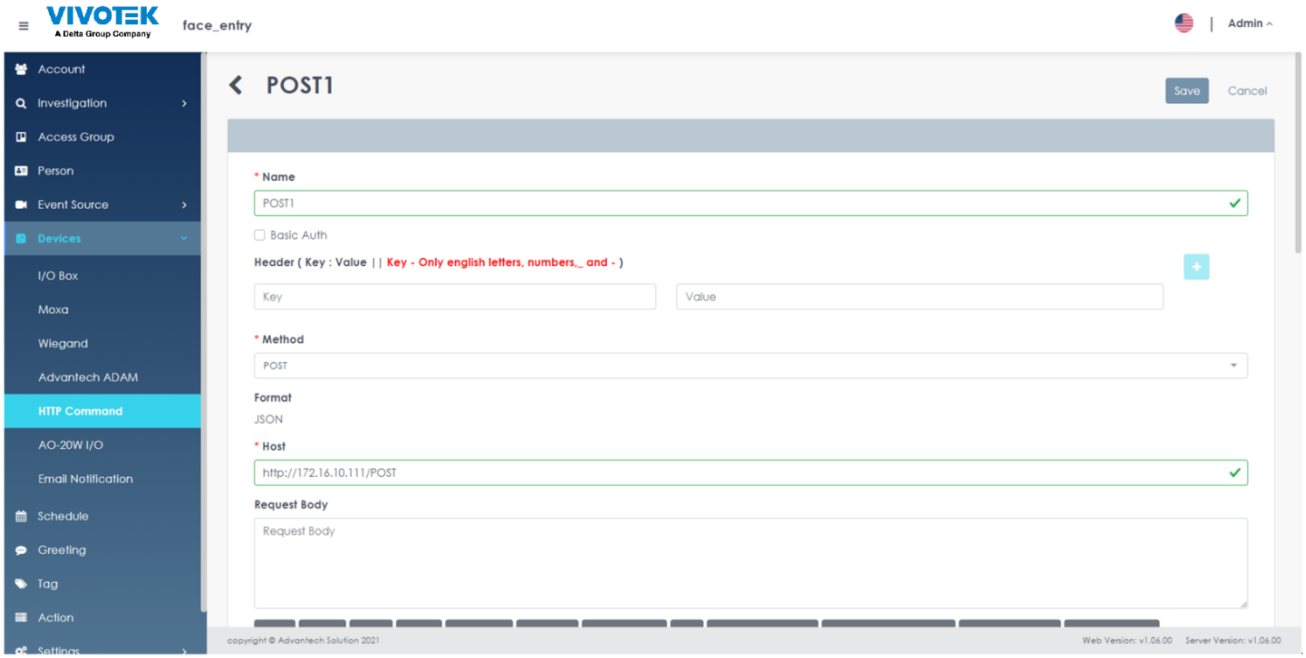


FIGURE 2.78 Device - create HTTP Command

11. On the "Create HTTP Command" menu, enter the new HTTP Command data message.

a. Name ➡ self-defined HTTP Command Name

b. Basic Authorization ➡ if authentication is required, you need to set the authentication account and password

c. Header ➡ (optional) HTTP header and Key value (multiple sets can be set)

d. Method Select ➡ HTTP data transfer method (GET or POST)

e. Request ➡ Please request the main HTTP message body

f. Format ➡(fixed) JSON format

g. Host location Target ➡ URL to which HTTP messages will be sent

12. Click "Save" to create HTTP Command data

2.9.6 AO-20W I/O

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login to Face Manager server with Administrator credentials

3. Navigate to the "Device" menu "➡AO-20W I/O", which will display all the created AO-20W I/O data

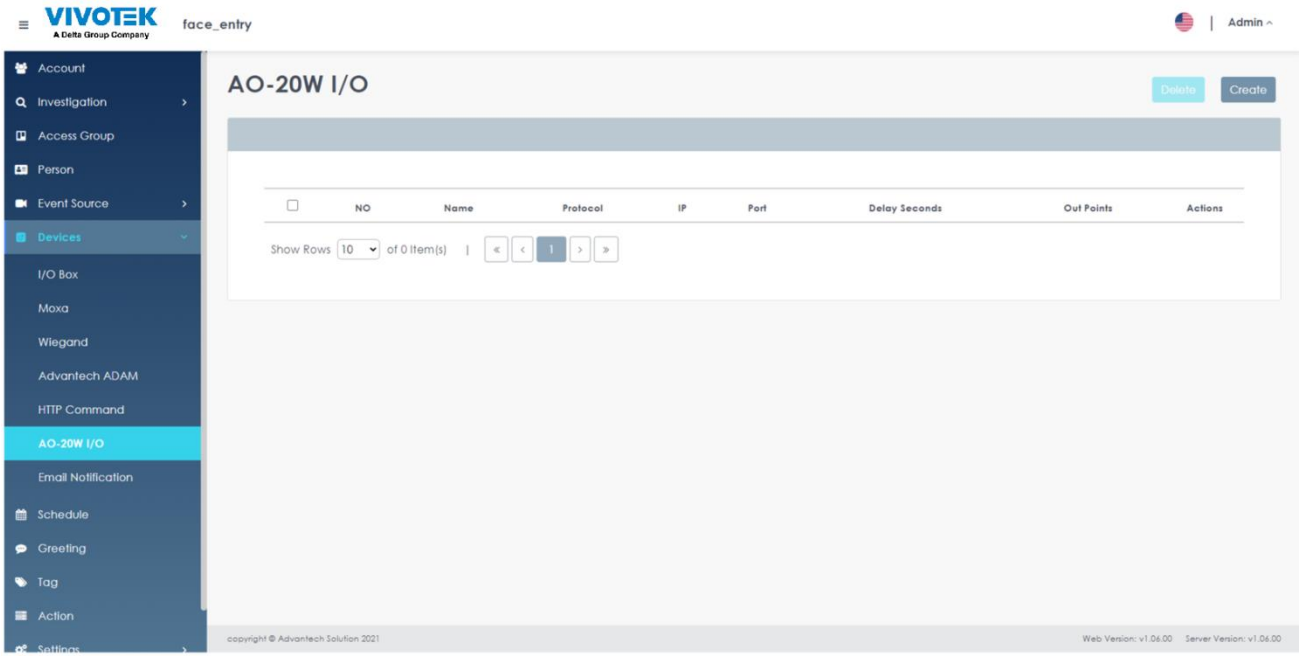


FIGURE 2.79 Device - AO-20W I/O list

4. To view the details of the AO-20W I/O, click on the "Details" ⋮ icon and select "Modify" to display the full details of the selected AO-20W I/O

5. Modify any required changes

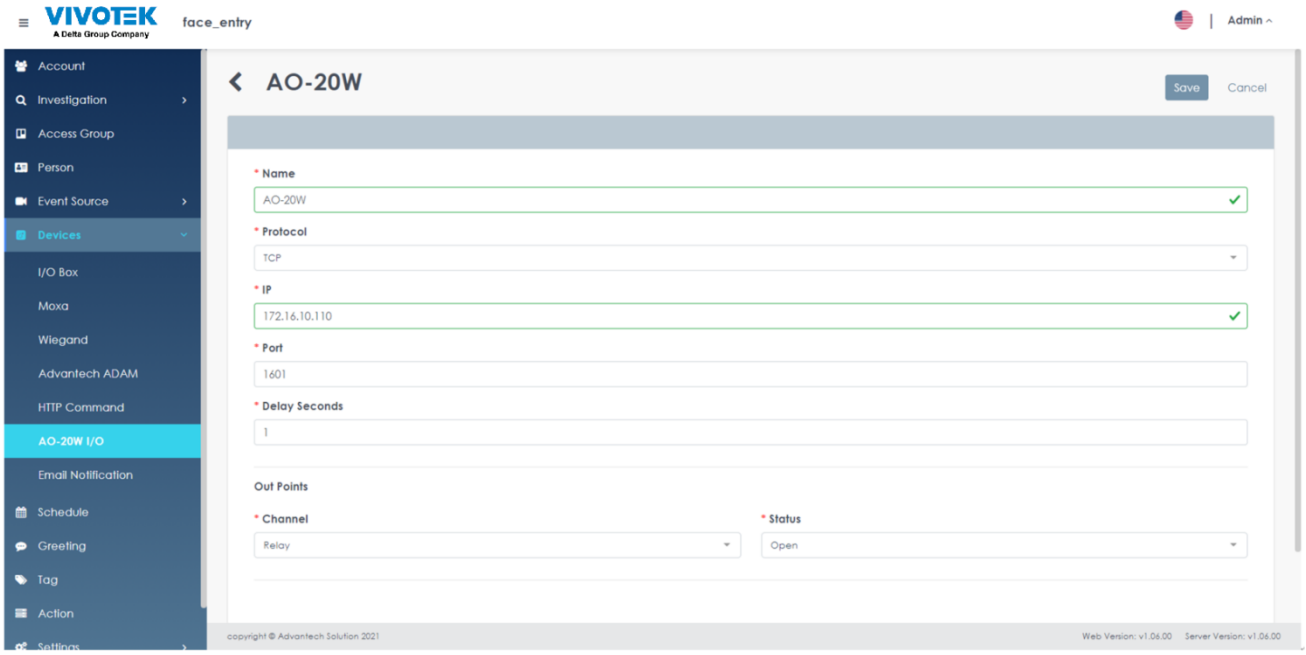


FIGURE 2.80 Device - AO-20W I/O details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon (⋮) and select Delete (Delete)
8. A pop-up window will appear on the screen, prompting the user to confirm the action

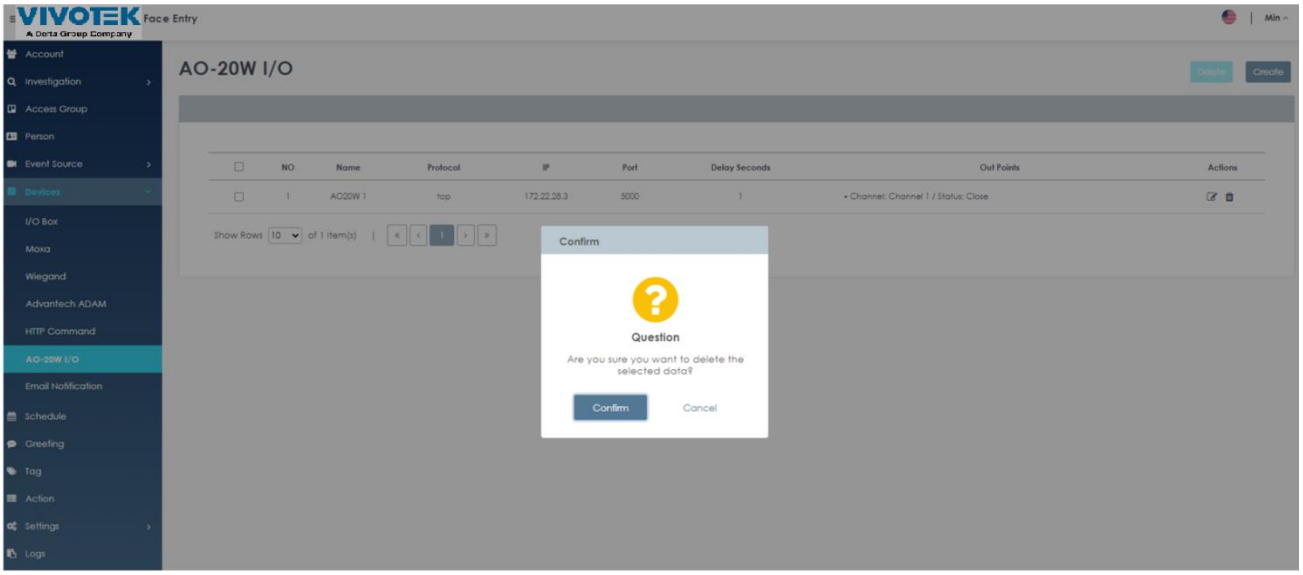


FIGURE 2.81 Device delete AO-20W I/O

9. Click "Confirm" to delete the selected AO-20W I/O data.
10. To add AO-20W I/O data, click the "+ Create" button (+ Create).

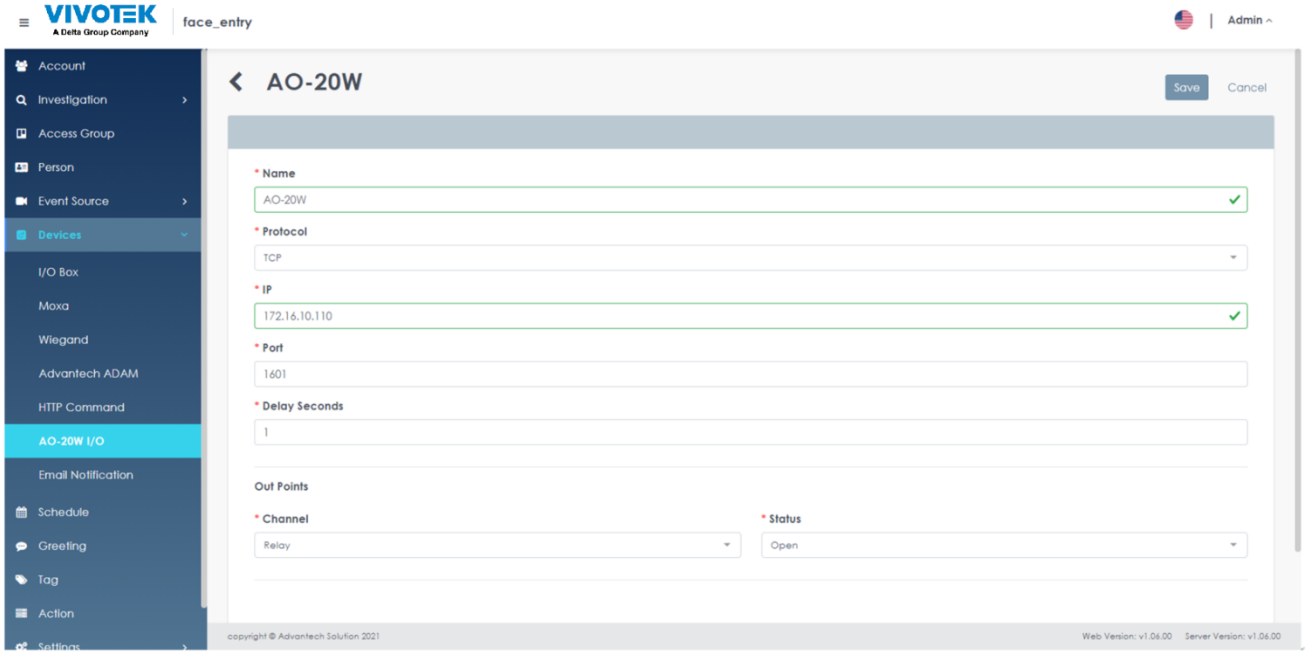


FIGURE 2.82 Device - create AO-20W I/O

11. On the "Create AO-20W I/O" menu, enter the new AO-20W I/O data message.
    a. Name ➡ Self-defined AO-20W I/O name
    b. Protocol Setting ➡ Select the protocol (TCP Client / UDP Client) for connecting to AO-20W I/O.
    c. IP setting ➡ setup IP address of the connection of AO-20W I/O
    d. Port Setting ➡setup port number to which AO-20W I/O is connected
    e. Delay seconds Setting ➡ setup delay time to maintain AO-20W I/O after each action trigger state change, after the delay time, the AO-20W I/O will return to the original state.

Remark

- The original state of AO-20W I/O depends on the trigger state, if the trigger state is "on", the original state is "off", and vice versa if the trigger state is "off", the original state is "on".

    f. Trigger position Set the DO output (Channel 1 / Channel 2) and trigger status (on/off) of ➡the AO-20W I/O.

12. Click "Test" to test if the IP and port can be properly connected to the AO-20W I/O. If the test fails, the device data cannot be saved.
13. Click "Save" to create AO-20W I/O data

2.9.6 AO-20W WG

14. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

15. Login to Face Manager server with Administrator credentials

16. Navigate to “Devices” menu ➡ “AO-20W WG”, a list of all created Wiegand will be displayed.

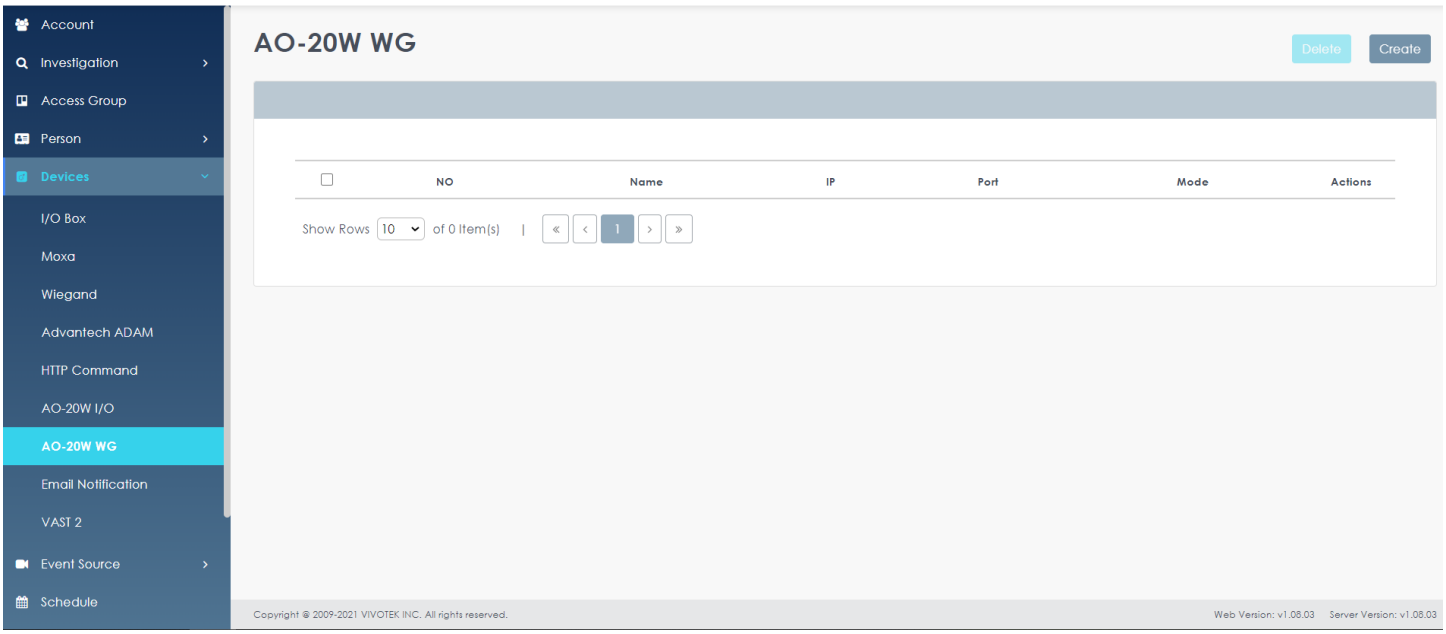


FIGURE 2.83 Device – AO-20W list

17. To view the Wiegand details, click on the "Details" ⋮ icon and select "Modify" to display the full details of the selected Wiegand

18. On the “Create Wiegand” menu, enter the new Wiegand information:

    a. Name ➡ A user-friendly name to identify this device.

    b. IP ➡ The device’s IP address.

    c. Port ➡ The device’s communication port.

    d. Mode ➡ Corresponds to the Card technology (iClass or Mifare) and Wiegand bits (26 or 34) format that the converter will output.

FIGURE 2.84 Device - Wiegand details

19. Click "Test" will pop up a test window for sending test card NO to test whether the IP and Port can connect to the Wiegand correctly

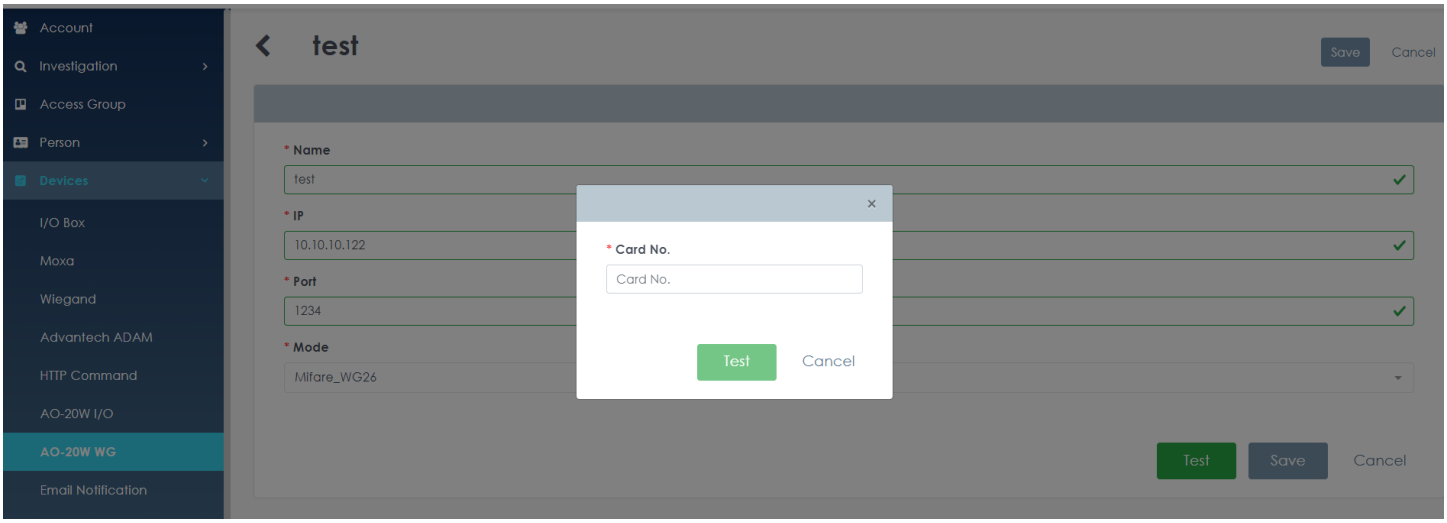


FIGURE 2.85 Device Test

20. Click "Save" to apply changes
21. To Delete a profile, click on the “Profile Details” icon ( ), and select Delete (Delete).
22. A pop-up window will appear on-screen prompting the user to confirm the action.
23. Click on “Confirm” to delete the selected Wiegand (s).
24. To add a new Wiegand, click on the “+Create” button (+ Create).

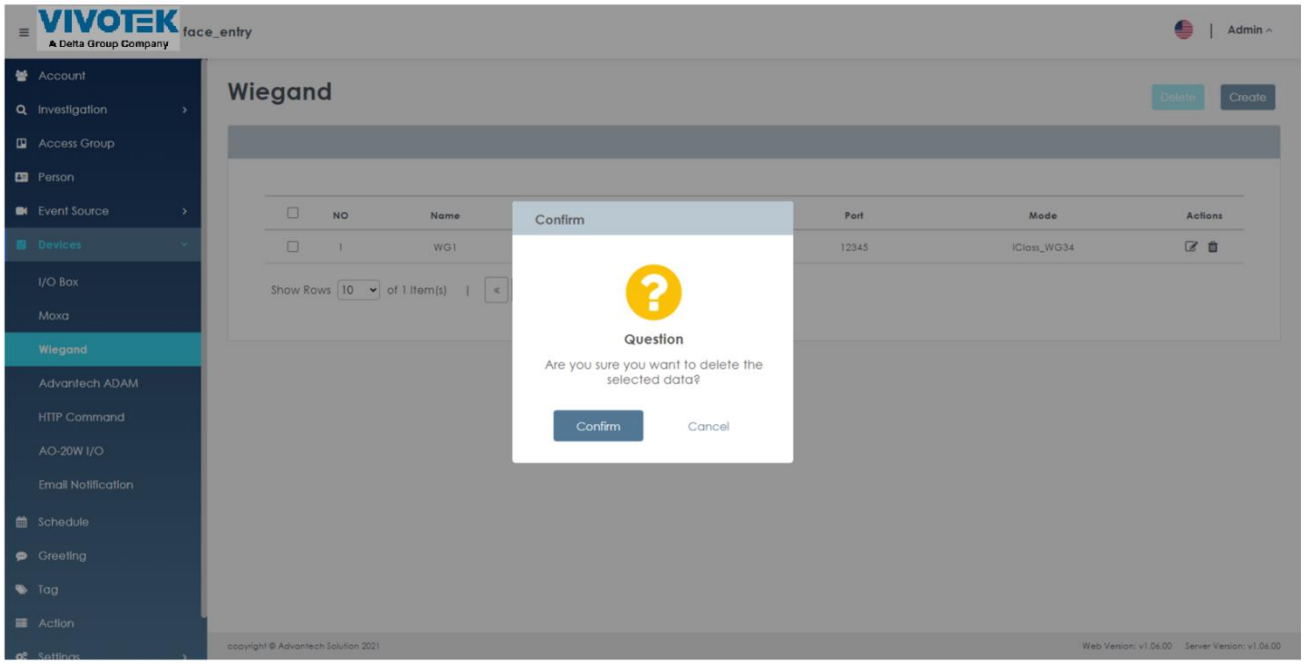


FIGURE 2.86 Device delete Wieand

2.9.6 Email Notification

If a specific person needs to be notified when a specific event is detected, Face Manager provides a simple setup method that customizes the notification title, content, and mailbox of the person to be notified to meet the requirements.

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login to Face Manager server with Administrator credentials

3. Navigate to the "Devices" menu "➡Email Notification", which will show all the created Email Notification data

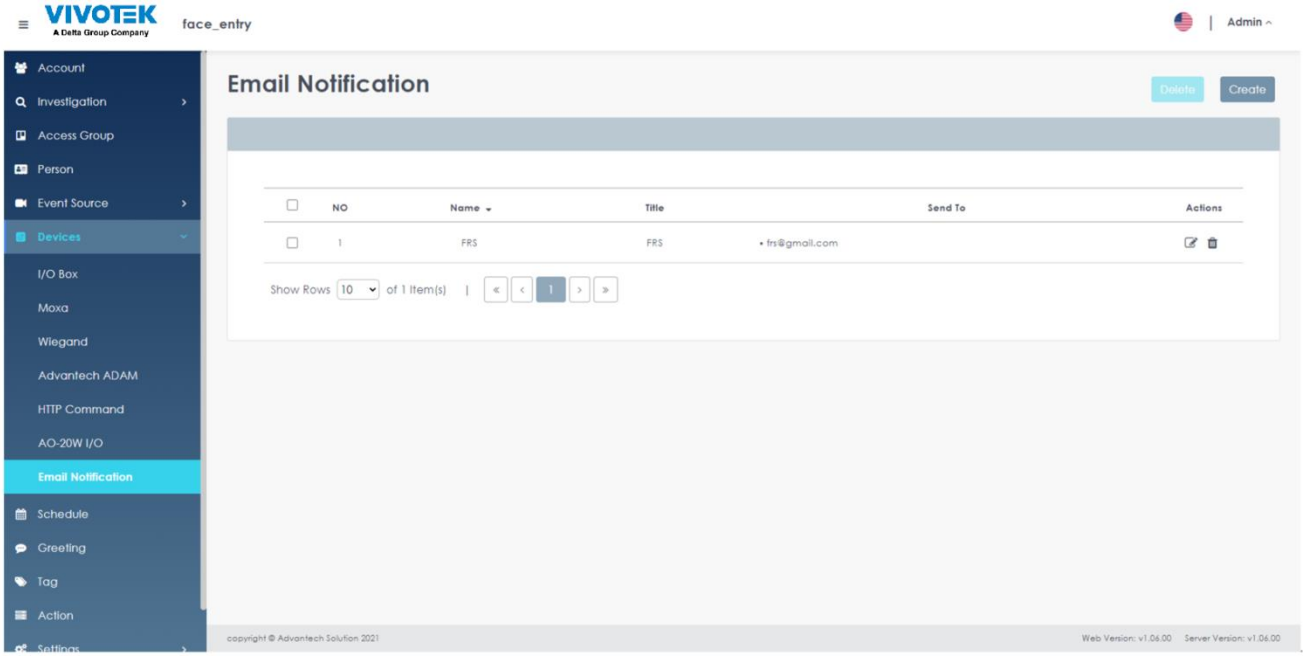


FIGURE 2.87 Device - Email Notification list

4. To view the details of an Email Notification, click on the "Details" ⋮ icon and select "Modify", which will display the full details of the selected Email Notification
5. Modify any required changes

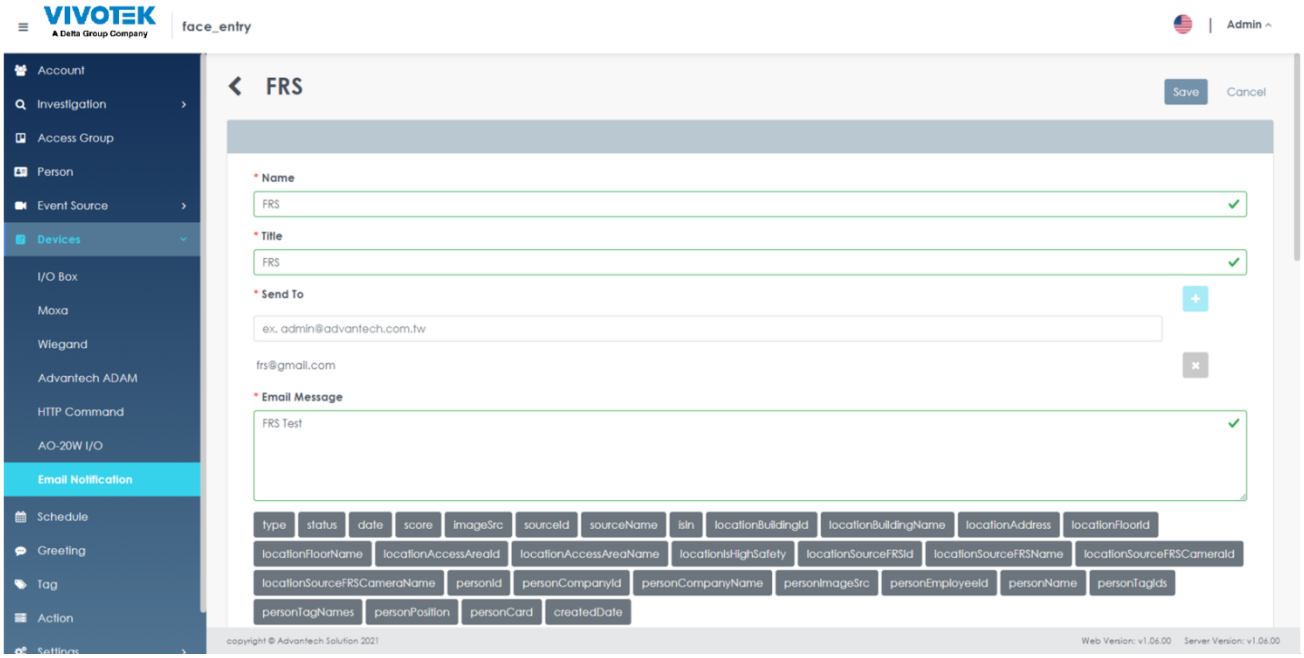


FIGURE 2.88 Device - Email Notification details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon (⋮ and select Delete (🗑 Delete
8. A pop-up window will appear on the screen, prompting the user to confirm the action

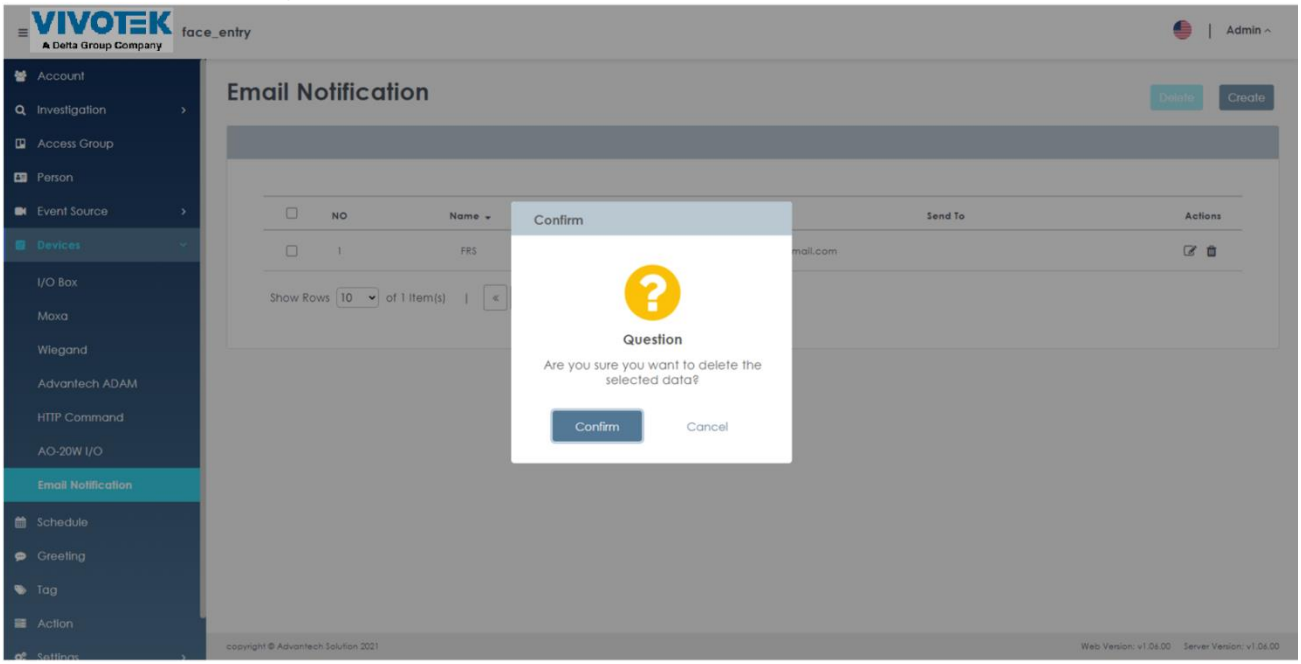


FIGURE 2.89 Device delete Email Notification

9. Click "Confirm" to delete the selected Email Notification data
10. To add Email Notification data, click the "+ Create" button (+ Create).

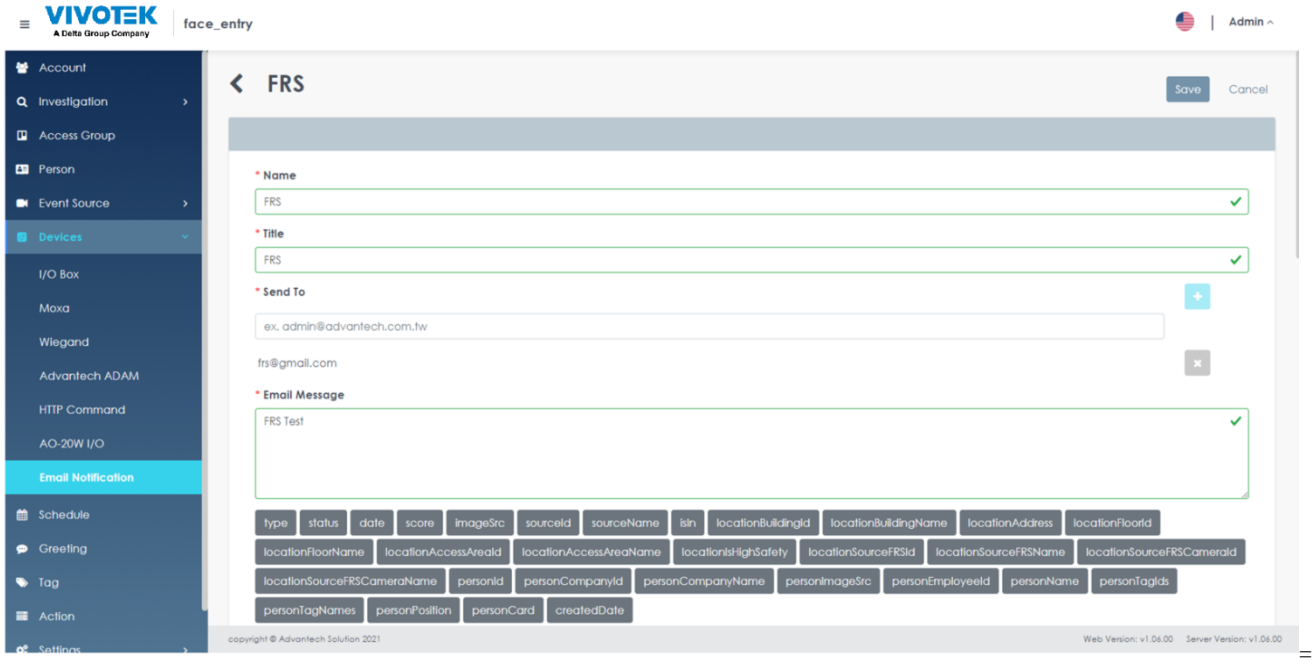


FIGURE 2.90 Device - create Email Notification

11. On the "Create Email Notification" menu, enter a new Email Notification data message.
    a. Name ➡ Self-defined Email Notification Name

b. Notification Subject Title ➡ Self-defined notification subject title

c. Mailing Address ➡The email address of the person to be notified (multiple groups can be set)

d. Mail Content ➡ Self-defined Notification mail content

12. Click "Save" to create Email Notification data

2.10 Actions Trigger

After adding devices or commands to the Face Manager server that should be triggered, you must specify the conditions for when these actions are triggered (triggering rules).

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login to Face Manager server with Administrator credentials

3. Navigate to the "Actions Trigger" menu, which will show all the created actions trigger data

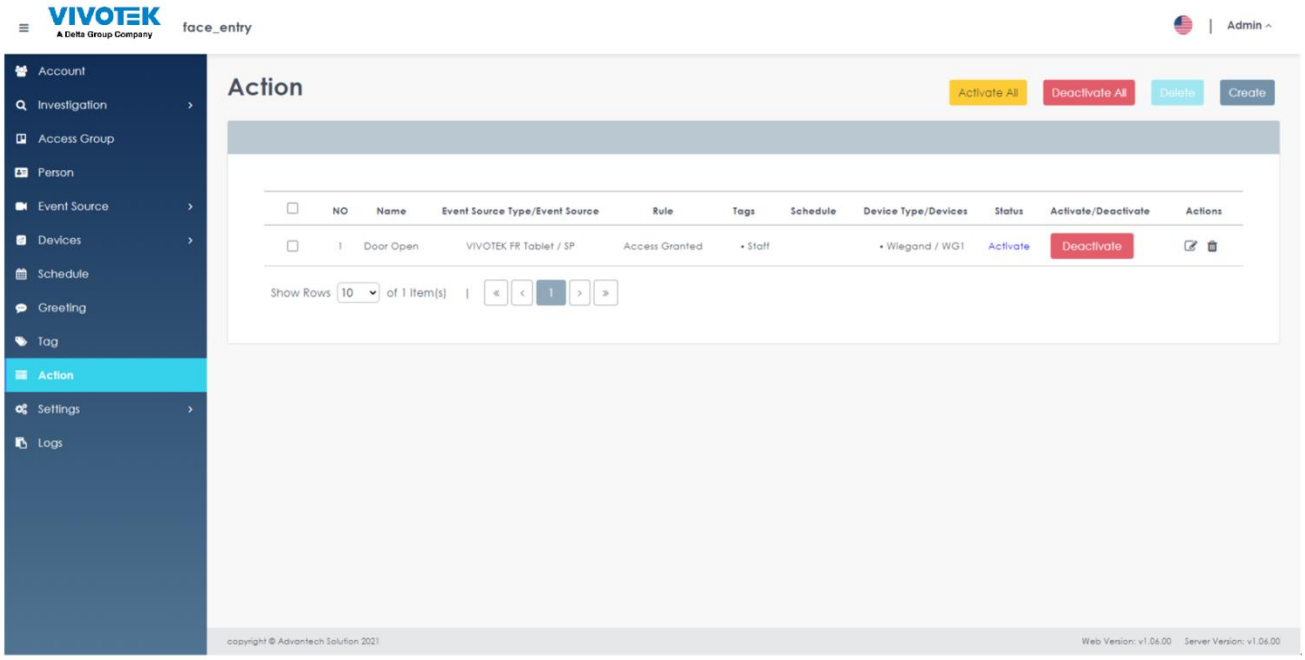


FIGURE 2.91 Action List

4. To view the details of the triggered image, click on the "Details" icon and select "Modify", full details of the selected image source will be displayed

5. Modify any required changes

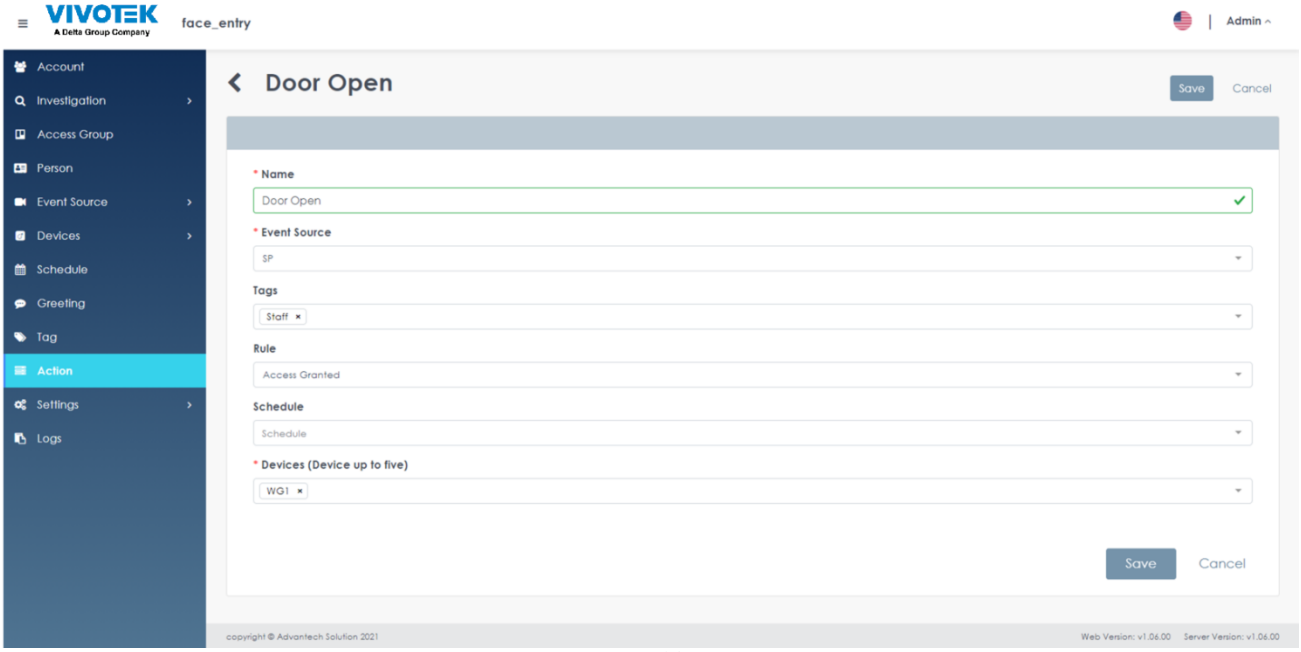


FIGURE 2.92 ACTION - details

6. Click "Save" to apply changes
7. To delete data, click on the "Details" icon (⋮ and select Delete (🗑 Delete
8. A pop-up window will appear on the screen, prompting the user to confirm the action

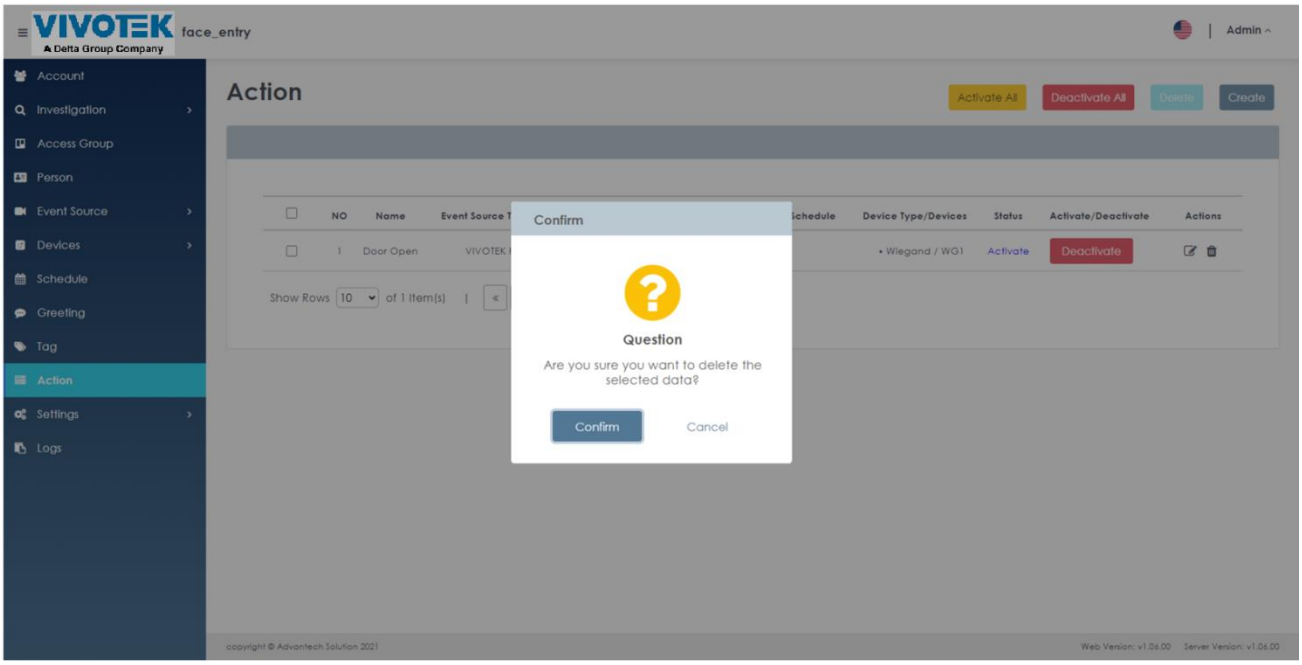


FIGURE 2.93 Delete ACTION

9. Click "Confirm" to delete the selected trigger data
10. To add a trigger to the data, click the "+ Create" button (+ Create).

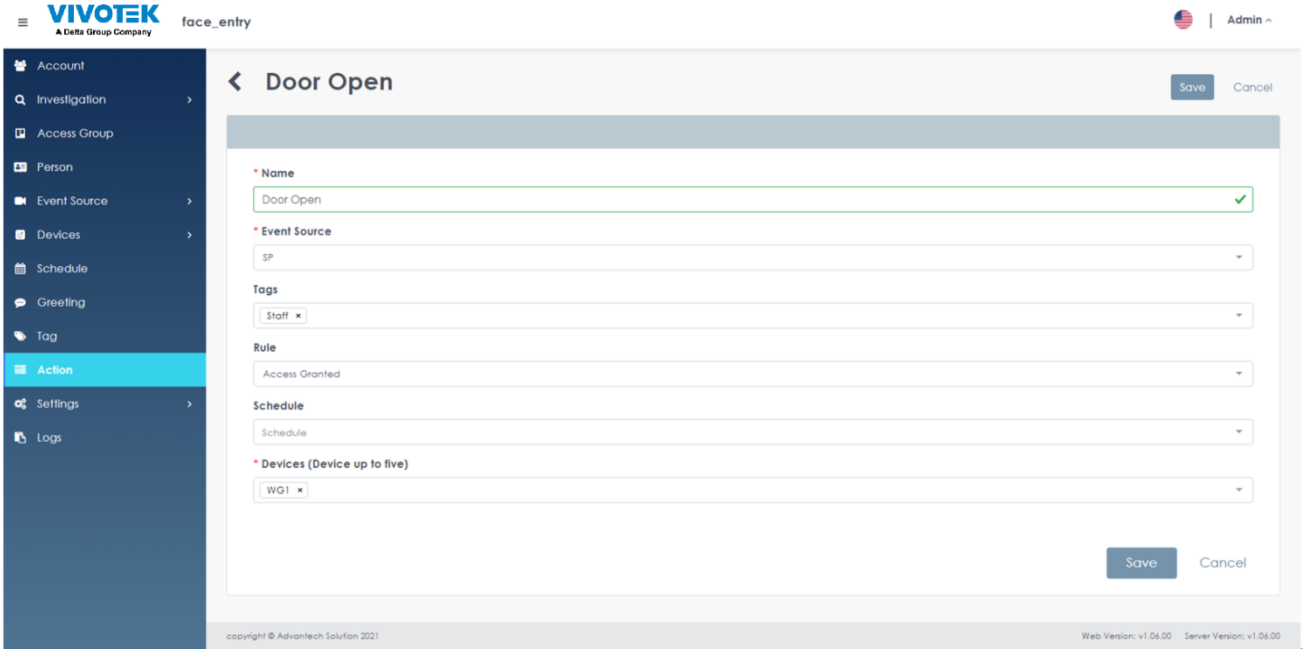


FIGURE 2.94 Create ACTION

11. On the "Create Trigger Action" menu, enter the new trigger action data message.
    a. Trigger Action Name ➡ Self-defined Trigger Action Name
    b. Image Source ➡ Select the configured camera or tablet whose face recognition results will be used to trigger this rule
    c. Rule ➡ (Optional) The type of face recognition event used to trigger this rule.
    d. Face Tag/ Label ➡ (Optional) Face tag/ label used to trigger this rule

Face Type		Person Group	Rule Definition
Known	+	No group selected	Trigger event rule when any system enrolled person is detected, regardless of face group affiliation
Known	+	With specific group(s) selected	Trigger event rule only when a member of a specific face group(s) is detected i.e. : trigger only when VIP face group members are detected
Unknown	+	No group selected	Trigger event rule when any unregistered person's face is detected
Unknown	+	With specific group(s) selected	Trigger event rule only when a person that's not part of a specific face group(s) is detected i.e. : trigger only when non VIP face group members are detected

    e. Scheduling ➡(optional) The selected rule will be executed during the scheduling time, if no schedule is selected, the rule will continue to be executed
    f. Device Auxiliary device or HTTP command➡(up to 5 per rule)

12. Click "Save" to create a trigger for the action data

Remark

- The touch issue is set to "enable" or "disable" the action on demand after the setting is completed

2.11 System Admin Only

2.11.1 Face Recognition Settings

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to "Face Recognition Settings" in the "Settings" menu➡
4. Modify the "Face Settings" as required.
    a. "VAST FACE Report Synchronization Interval" ➡Frequency" value (expressed in minutes), used to define how long it takes for the VAST Face Manager to connect to a controlled FR device to obtain a face recognition event
5. Click "Save" to apply changes

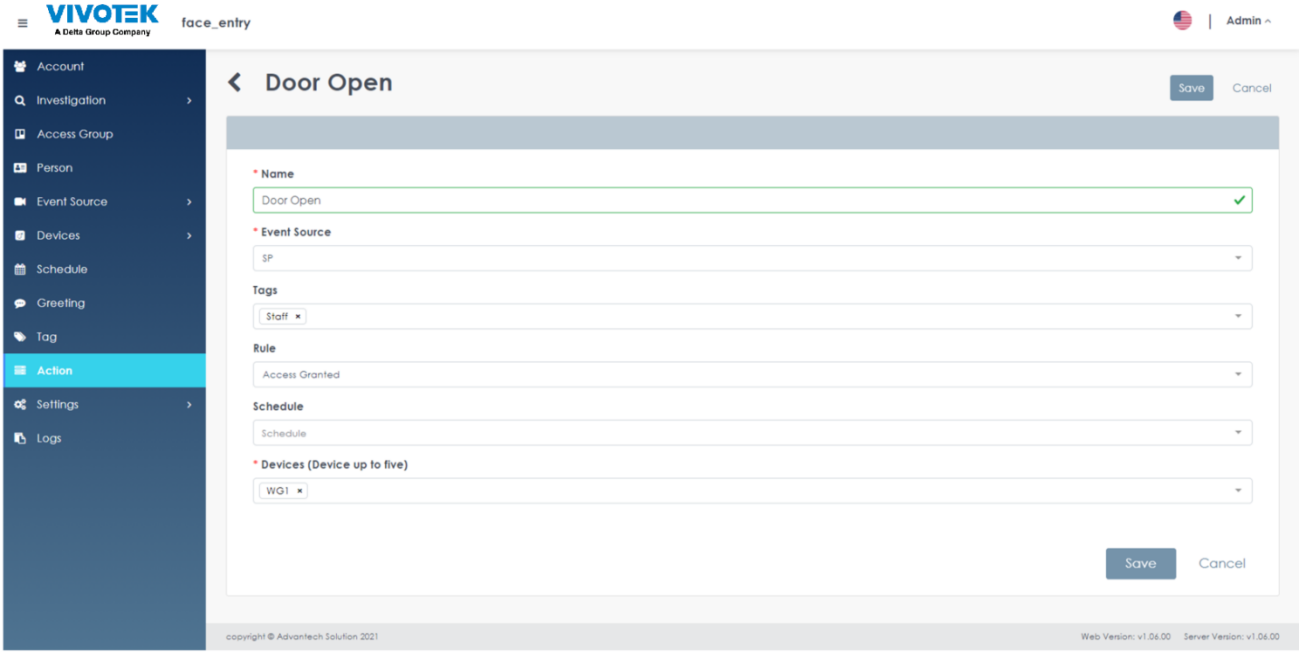


FIGURE 2.95 Face Manager Face Settings page

2.11.2 Face Recognition Engine Settings

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Settings" menu ➡"

4. Under "Face Recognition Engine Settings Settings", enter the following information.

    a. Protocol ➡ Select "HTTP"

    b. IP Address ➡ Enter VAST FACE Edge server IP address

    c. Port No. ➡ Enter 6075

    d. Account ➡ Enter name of the account created under "ADVANTECH VAST FACE Edge Creation User".

    e. Password ➡Enter password for the account created under "ADVANTECH VAST FACE Edge Creation User".

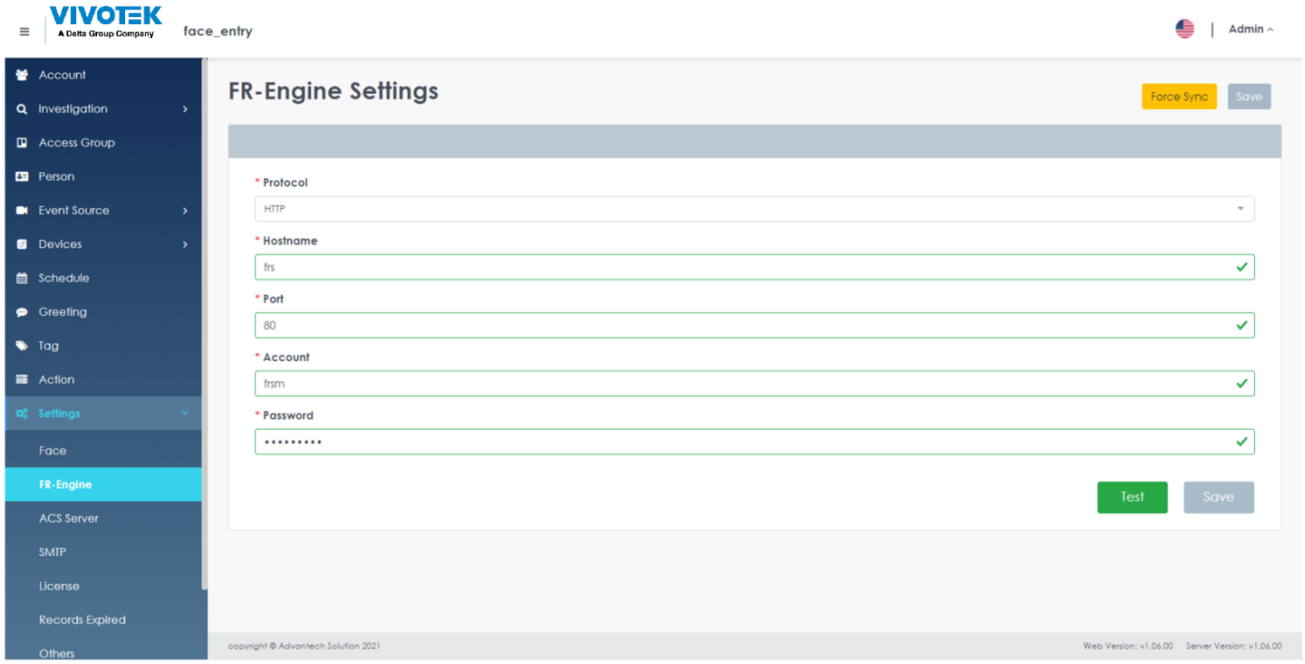


FIGURE 2.96 Face Manager FR Engine settings menu

5. Click "Save" to apply changes

2.11.3 ACS configuration

Remark

- If the Face Manager server will not be connected to an external third-party Access Control System (ACS), this step can be skipped and the user can follow the default configuration

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Settings" menu "➡ACS Server"
4. Under the ACS server settings, modify the card number range.
    a. Employee card number The ➡corresponding card number range will be used for the registered face data

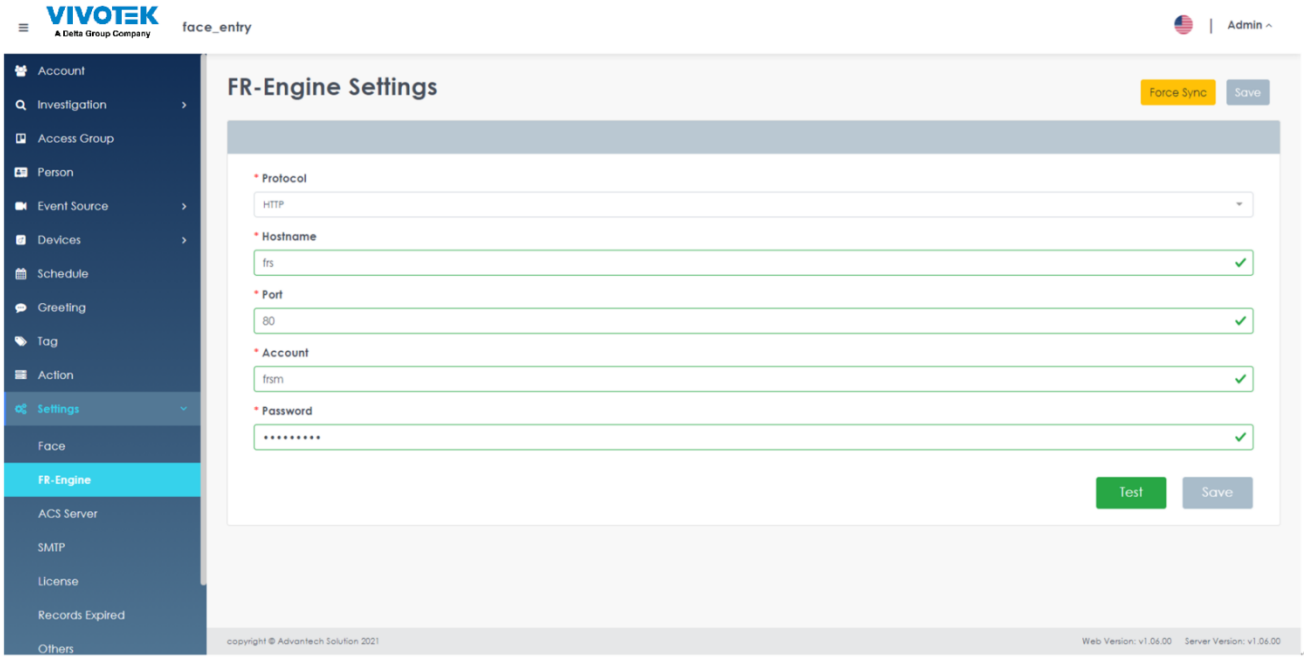


FIGURE 2.97 Face Manager server ACS Server Settings page

5. Click "Save" to apply changes

2.11.4 SMTP configuration

Remark

- If system users want to recover their account password via email, they must connect their SMTP (mail) server account to the VAST Face Manager server, or skip this step if they do not need this feature.

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to "Settings" menu "➡SMTP"

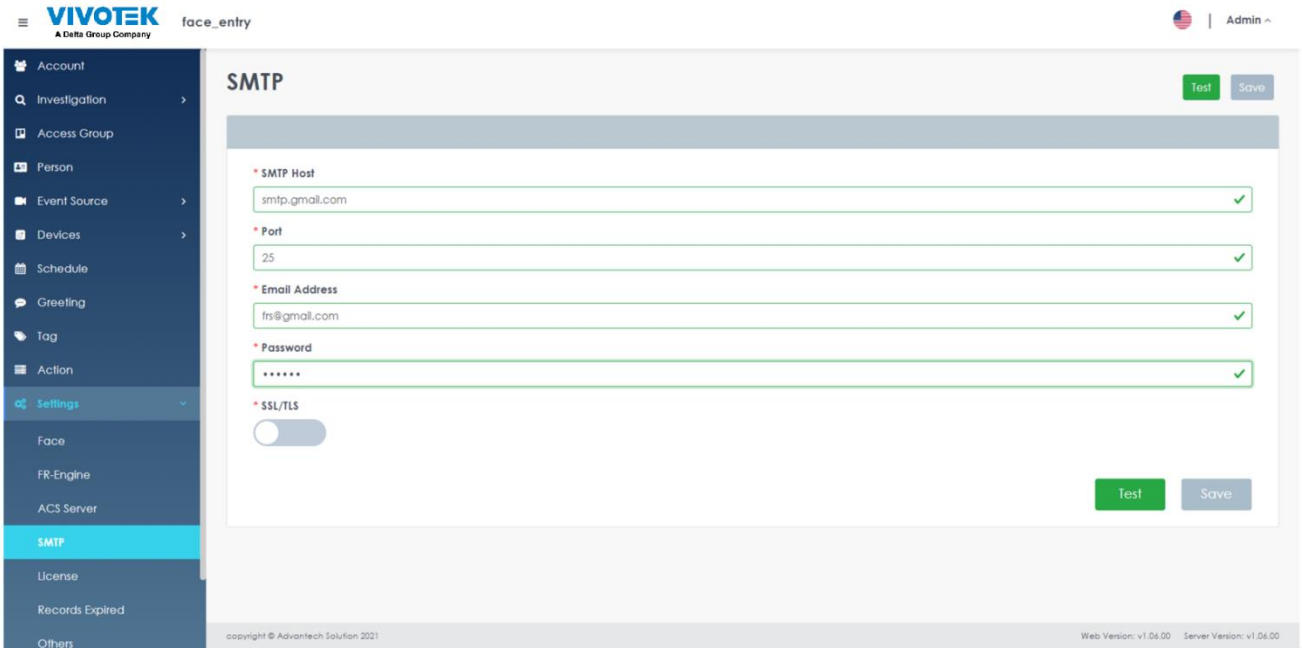


FIGURE 2.98 Face Manager server SMTP Settings page

4. Click on the "SMTP" server menu to provide the following information.
   a. Host Location Enter the specified➡ SMTP server IP address/host name
   b. Port Number Enter the port number of the ➡specified SMTP server
   c. Email ➡Enter the specified secondary email address
   d. Password ➡Enter the password for the specified secondary email address
   e. SSL / TLS If ➡SMTP requires SSL / TLS connection, please check the box
5. Click on "Test" and enter the address of the incoming test email, which can be used as a confirmation that SMTP emails have been configured correctly
6. Click "Save" to apply changes

2.11.5 Registering a Face Manager Server license

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Settings" menu ➡License" and click the "+ Register License Online" button

4. Enter the Face Manager license key and select the MAC address associated with the license key.
5. Click "Save" to register a license

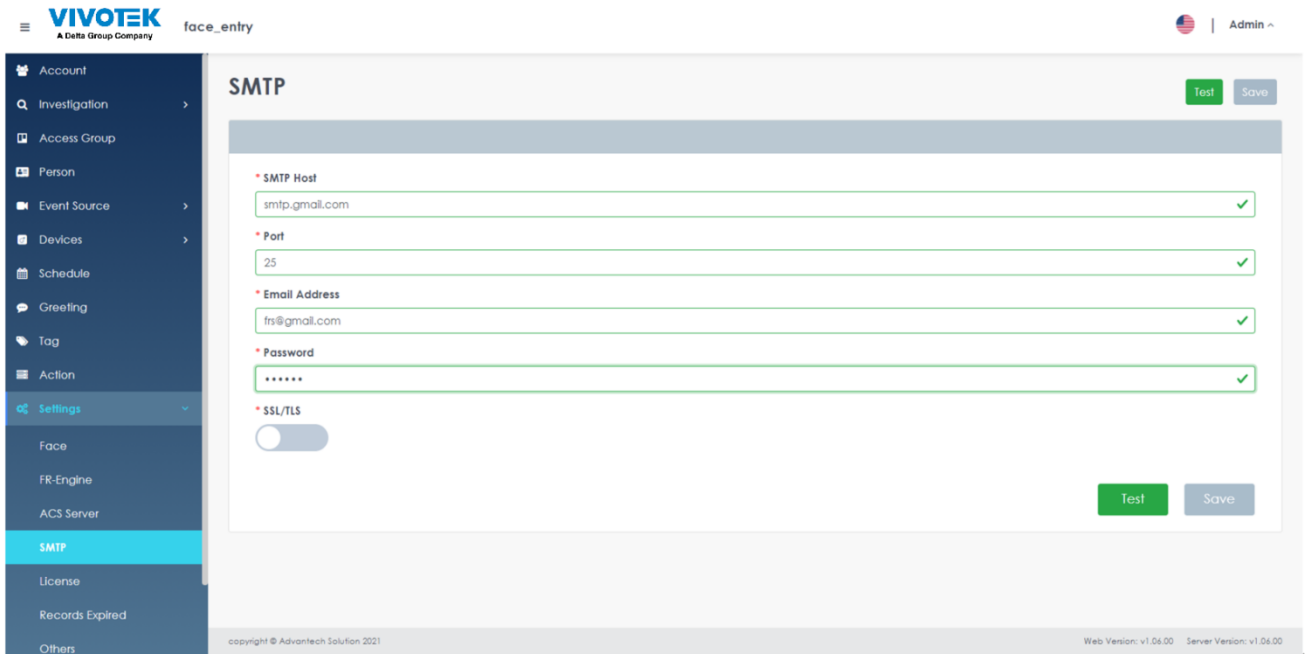


FIGURE 2.99 Face Manager license registration menu

Remark

- Internet is required to enable the license key

6. If registration is successful, a new license will be added to the "License" menu

2.11.6 Record Retention Settings

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Settings" menu➡ "Record Retention Settings"
4. Modify the "Record Retention Settings" as required.
    a. "Survey Data Retention Days" ➡(unit: days), used to define how many days the survey data will be retained and then automatically deleted
5. Click "Save" to apply changes

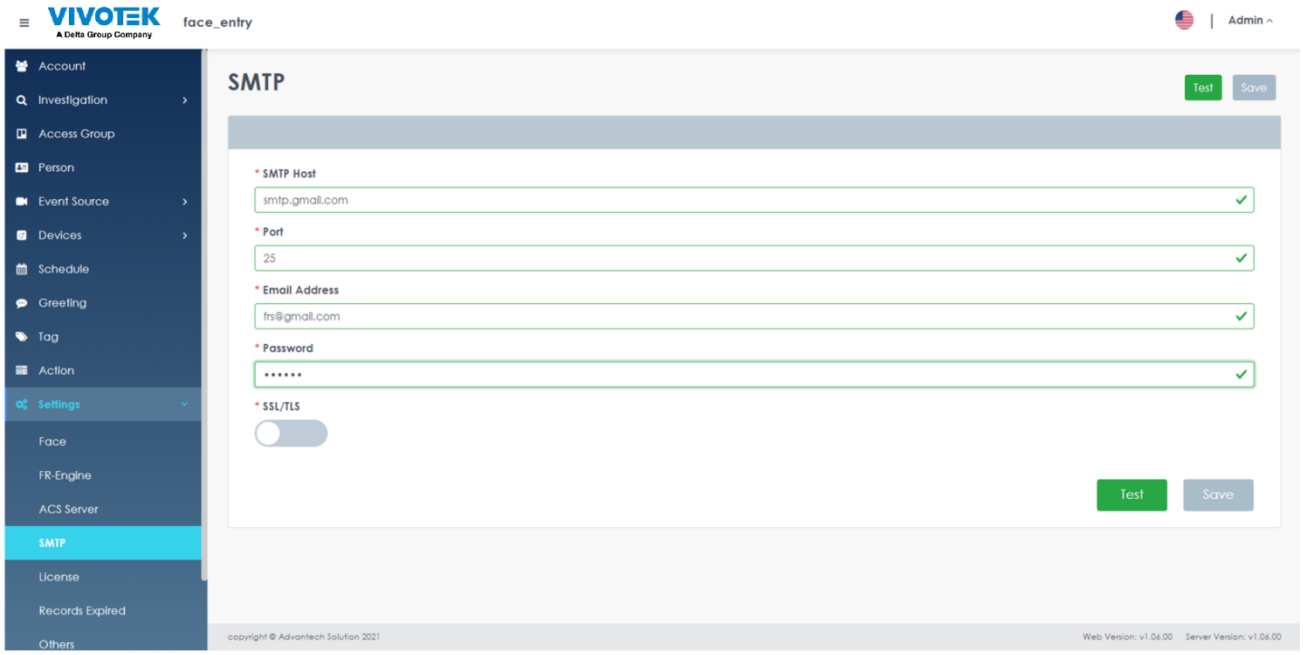


FIGURE 2.100 Face Manager Records Expired Settings page

2.11.7 Other settings

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Settings" menu➡ "Other Settings"
4. Set by demand.
    a. "Upload T&C PDF files"➡ You can upload T&C PDF files by yourself and view the uploaded files
    b. "Location"➡sets the building, floor and company information to be used

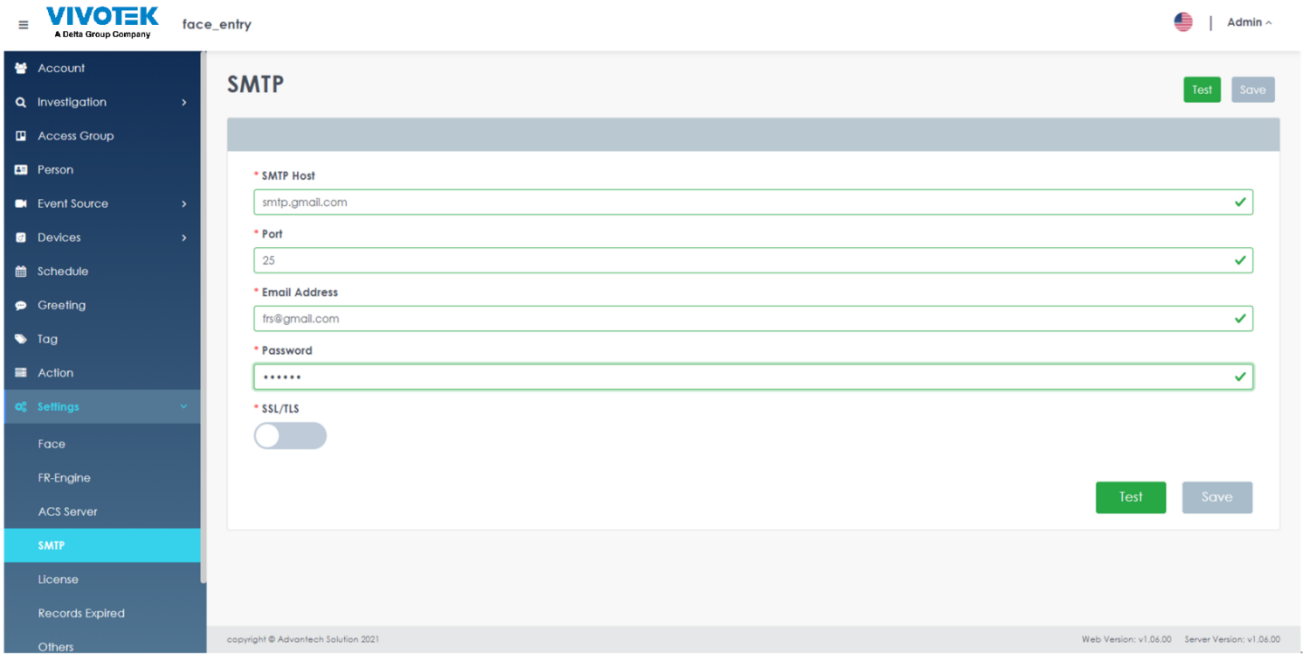


FIGURE 2.101 Face Manager Other Settings page

2.11.8 Notification Settings

When the system operates the forced sync function or when the connection to the image source fails, you can set up a notification to inform a specific person of the system abnormalities.

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (i.e. http://192.168.1.152:6073), which will display the Face Manager server login page
2. Login to Face Manager with System Admin credentials
3. Navigate to the "Settings" menu➡ "Notification objects", which will display all the created notification data

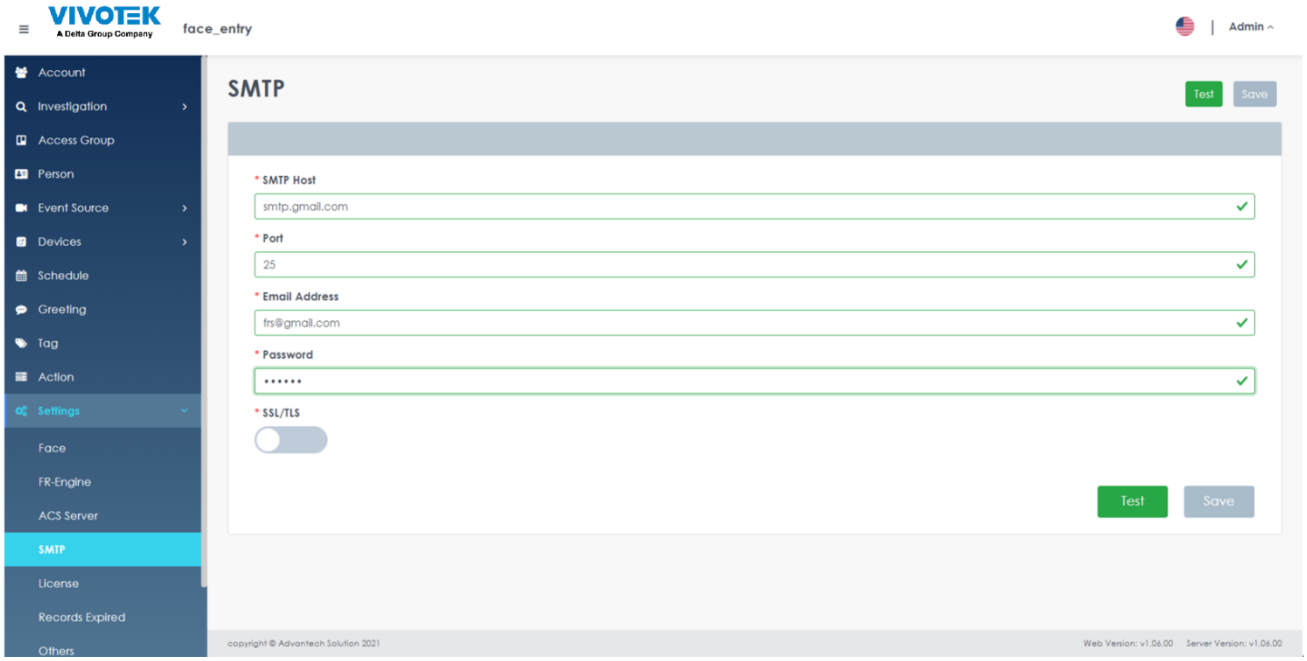


FIGURE 2.102 Face Manager Notification Setting page

4. In order to view the details of the notification recipient, click on the "Details" ⋮ icon and select "Modify", which will display the full details of the selected notification recipient
5. Modify any required changes

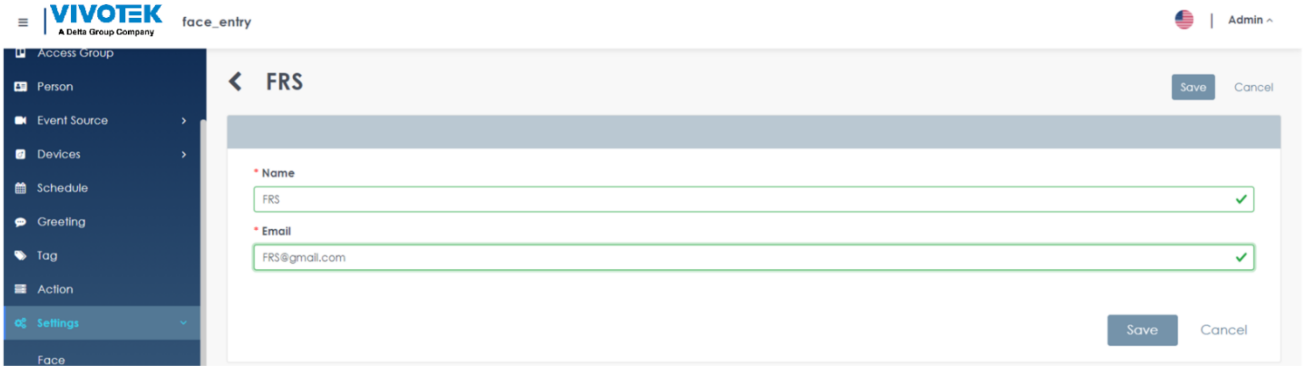


FIGURE 2.103 Face Manager Notification Edit

6. Click "Save" to apply changes

7. To delete data, click on the "Details" icon (⋮) and select Delete (Delete)
8. A pop-up window will appear on the screen, prompting the user to confirm the action

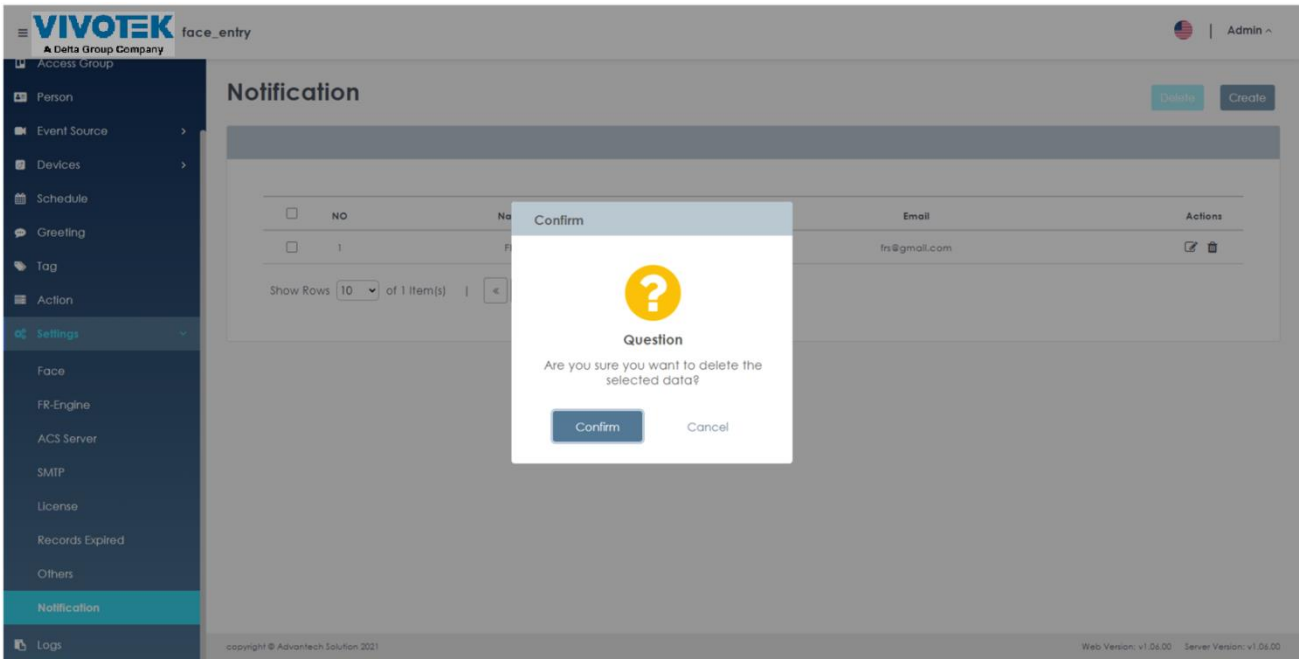


FIGURE 2.104 Face Manager Notification Delete

9. Click "Confirm" to delete the selected notification recipients
10. To add a new notification object, click the "+ Create" button (+ Create).

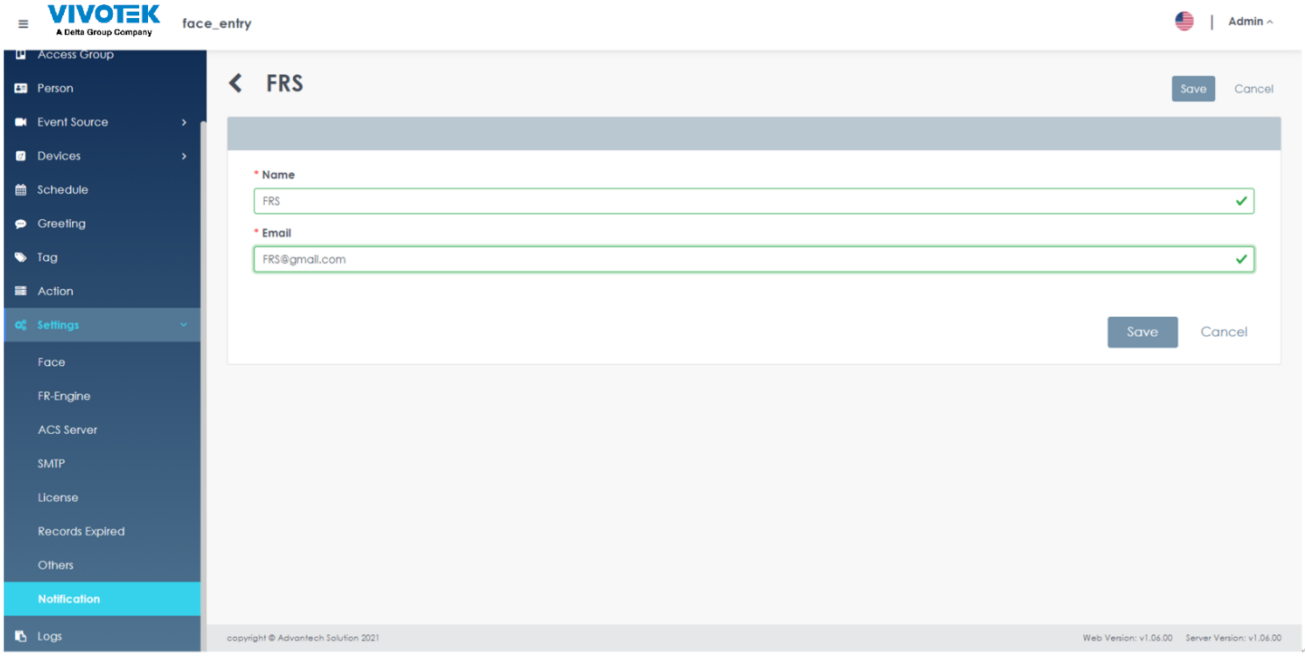


FIGURE 2.105 Face Manager Notification Create

11. On the "Notification recipients" menu, enter a new notification recipient data message.

a. Name Name of Notification Recipient➡

b. Email Email address of the➡person who wants to send the notice

12. Click "Save" to create notification recipients

2.12 Logs Management (System Admin Only)

1. On Windows OS PC, open Google Chrome and navigate to the Face Manager server IP address, port number 6073 (http://192.168.1.152:6073), which will display the "Face Manager Server Login" page

2. Login to Face Manager server with System Admin credentials

3. Navigate to the "Logs" menu All system logs will be displayed➡

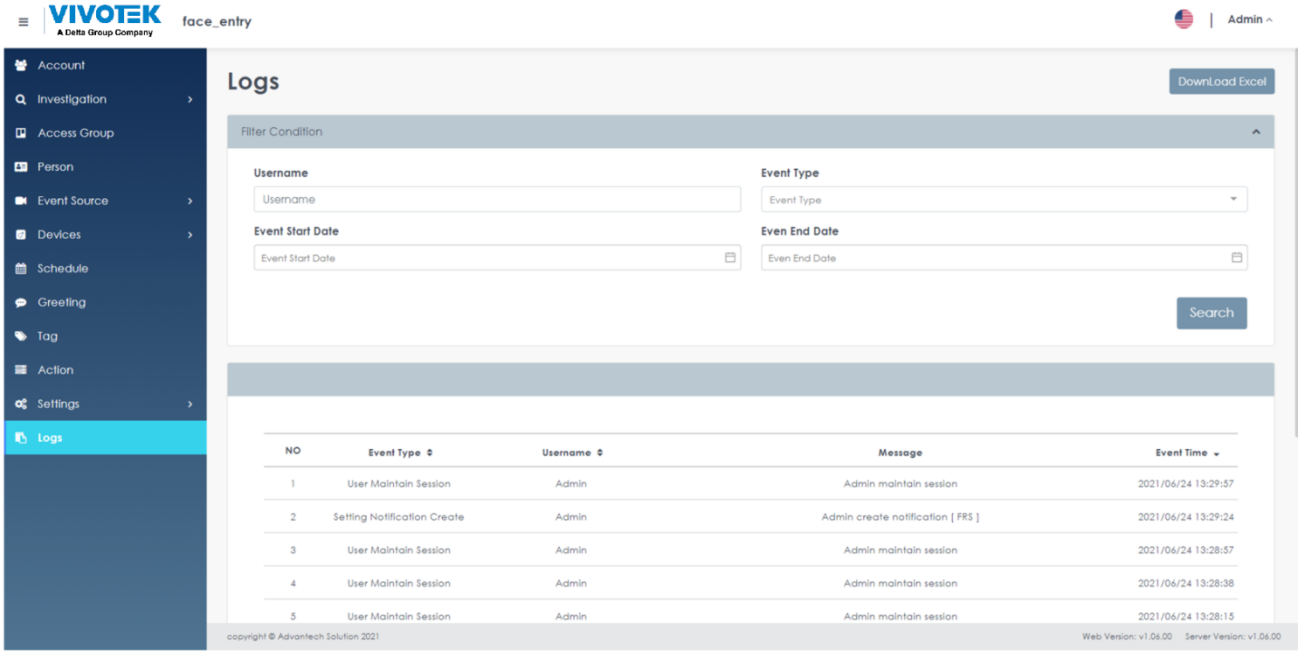


FIGURE 2.106 FIGURE 3.86 Logs List

4. Use the filter to filter the result range by user name, event type, start date or end date

5. Click the "Search" button

6. Only logs that meet the filter criteria will be displayed on the screen

7. To export logs, click the "Export to Excel" button and it will export to your PC